iPECS

User Manual

ES-2026 Advanced Smart FE Switch
ES-2026P Advanced Smart FE PoE Switch
ES-2024G Advanced Smart GE Switch
ES-2024GP Advanced Smart GE PoE Switch

LG-ERICSSON

USER MANUAL

iPECS ES-2000 Series

ES-2026 ADVANCED SMART 26-PORT FE SWITCH

Layer 2 Advanced Smart Switch
with 24 10/100BASE-TX (RJ-45) Ports,
and 2 Gigabit Combination Ports (RJ-45/SFP)

ES-2026P ADVANCED SMART 26-PORT FE POE SWITCH

Layer 2 Advanced Smart Switch
with 24 10/100BASE-TX (RJ-45) PoE Ports,
and 2 Gigabit Combination Ports (RJ-45/SFP)

ES-2024G ADVANCED SMART 24-PORT GE SWITCH

Layer 2 Advanced Smart Switch
with 24 10/100/1000BASE-T (RJ-45) Ports,
and 4 Gigabit Shared Ports (SFP)

ES-2024GP ADVANCED SMART 24-PORT GE POE SWITCH

Layer 2 Advanced Smart Switch
with 24 10/100/1000BASE-T (RJ-45) PoE Ports,
and 4 Gigabit Shared Ports (SFP)

ES-2026 ES-2026P
ES-2024G ES-2024GP
E062011/ST-R05
149100000041A

ABOUT THIS GUIDE

PURPOSE This guide gives specific information on how to operate and use the management functions of the switch.

AUDIENCE The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

CONVENTIONS The following conventions are used throughout this guide to show information:



NOTE: Emphasizes important information or calls your attention to related features or instructions.



CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.



WARNING: Alerts you to a potential hazard that could cause personal injury.

NOTICE OF CHANGES LG-Ericsson reserves the right to change specifications at any time without notice.

RELATED PUBLICATIONS The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch:

The *Installation Guide*

Also, as part of the switch's software, there is an online web-based help that describes all management related features.

REVISION HISTORY

This section summarizes the changes in each revision of this guide.

JUNE 2011 REVISION

This is the fifth version of this guide. This guide is valid for software release v1.2.0.12. It includes information on the following changes to the web pages or command line interface:

- Updated descriptive text for port security (see "Configuring Port Security" on page 187.

JANUARY 2011 REVISION

This is the fourth version of this guide. This guide is valid for software release v1.2.0.8. It includes information on the following changes:

- Updated Table 3, "Web Page Configuration Buttons," on page 36.
- Updated Table 4, "Switch Main Menu," on page 39.
- Updated the parameter list in "Setting the Time Zone" on page 60.
- Updated the Command Usage section and Parameter list in "Resetting the System" on page 63.
- Updated the Command Usage section and Parameter list under "Configuring by Port List" on page 65.
- Updated Table 5, "Port Statistics," on page 71.
- Updated the Parameter list in "Configuring a Static Trunk" on page 78.
- Added the section for "Configuring Trunk Mirroring" on page 89.
- Updated the Parameter list in "Configuring VLAN Groups" on page 95.
- Updated the Parameter list in "Adding Static Members to VLANs" on page 96.
- Updated the Command Usage section and Parameter list in "Storm Control Configuration" on page 123.
- Updated the Command Usage section in "Setting the Default Priority for Interfaces" on page 125.
- Updated the Parameter list in "Configuring Remote Logon Authentication Servers" on page 163.
- Updated the Parameter list in "Configuring User Accounts" on page 166.
- Added information about LLDP-MED in "Link Layer Discovery Protocol" on page 205.
- Updated the Parameter list in "Setting LLDP Timing Attributes" on page 206.

- Updated the Parameter list in "Configuring LLDP Interface Attributes" on page 208.
- Added the section "Configuring LLDP Interface Civic-Address" on page 211.
- Updated the Parameter list in "Displaying LLDP Remote Port Information" on page 216.
- Updated Table 26, "Supported Notification Messages," on page 236.
- Updated information in "Setting the Switch's IP Address (IP Version 4)" on page 271.
- Updated the Parameter list in "Configuring IGMP Snooping and Query Parameters" on page 277.
- Updated the Parameter list in "Setting IGMP Snooping Status per Interface" on page 284.
- Added "Filtering and Throttling IGMP Groups" on page 290.

JULY 2010 REVISION

This is the third version of this guide. This guide is valid for software release v1.1.2.0. It includes information on the following changes:

- Updated corporate logo on cover pages, and on the switch image used in the management interface.

MAY 2010 REVISION

This is the second version of this guide. This guide is valid for software release v1.0.1.5. It includes information on the following changes to the web pages:

- Removed MAC Address > Learning Status page from the web interface.
- Added information on how to configure connection parameters for a dynamic trunk (see "Configuring a Dynamic Trunk" on page 80).
- Added description of "Admin Edge Status for all ports" in the STA interface configuration page (see "Configuring Interface Settings for STA" on page 113).
- Changed HTTP and HTTPS to function as mutually exclusive services (see "Configuring Global Settings for HTTPS" on page 172).
- Added information on how log messages are flushed from system memory or flash memory during cold or warm restart (see "Configuring Event Logging" on page 201).
- Added information on how to display log messages in system memory or flash memory using the web interface (see "Configuring Event Logging" on page 201).

- Updated Figure 118 on page 203.
- Updated Figure 124 on page 215.
- Added additional information about the parameters displayed for remote devices (see "Displaying LLDP Remote Port Information" on page 216).
- Updated Figure 127 on page 221.
- Updated Figure 130 on page 225.
- Removed the default IP address pool for switch clustering (see "Configuring General Settings for Clusters" on page 261).
- Added GNU "License Information" on page 303

DECEMBER 2009 REVISION

This is the first version of this guide. This guide is valid for software release v1.0.0.0.

CONTENTS

ABOUT THIS GUIDE 3
CONTENTS 7
FIGURES 13
TABLES 19

SECTION I GETTING STARTED 21

1 INTRODUCTION 23
Key Features 23
Description of Software Features 24
System Defaults 28
2 INITIAL SWITCH CONFIGURATION 31

SECTION II WEB CONFIGURATION 33

3 USING THE WEB INTERFACE 35
Navigating the Web Browser Interface 35
Home Page 35
Configuration Options 36
Panel Display 37
Showing Status Information 38
Main Menu 39
4 BASIC MANAGEMENT TASKS 47
Displaying System Information 47
Displaying Switch Hardware/Software Versions 48
Configuring Support for Jumbo Frames 50
Displaying Bridge Extension Capabilities 51
Managing System Files 52
Copying Files via HTTP 52
Saving the Running Configuration to a Local File 54

Setting The Start-Up File 55
Showing System Files 56
Setting the System Clock 57
Setting the Time Manually 57
Setting the SNTP Polling Interval 58
Specifying SNTP Time Servers 59
Setting the Time Zone 60
Displaying CPU Utilization 61
Displaying Memory Utilization 62
Resetting the System 63
5 INTERFACE CONFIGURATION 65
Port Configuration 65
Configuring by Port List 65
Configuring by Port Range 68
Displaying Connection Status 68
Configuring Local Port Mirroring 69
Showing Port or Trunk Statistics 71
Performing Cable Diagnostics 75
Trunk Configuration 77
Configuring a Static Trunk 78
Configuring a Dynamic Trunk 80
Displaying LACP Port Counters 85
Displaying LACP Settings and Status for the Local Side 87
Displaying LACP Settings and Status for the Remote Side 88
Configuring Trunk Mirroring 89
Saving Power 91
6 VLAN CONFIGURATION 93
IEEE 802.1Q VLANs 93
Configuring VLAN Groups 95
Adding Static Members to VLANs 96
7 ADDRESS TABLE SETTINGS 101
Setting Static Addresses 101
Changing the Aging Time 103
Displaying the Dynamic Address Table 104
Clearing the Dynamic Address Table 105

8 SPANNING TREE ALGORITHM 107
Overview 107
Configuring Global Settings for STA 108
Displaying Global Settings for STA 112
Configuring Interface Settings for STA 113
Displaying Interface Settings for STA 116
9 RATE LIMIT CONFIGURATION 119
10 STORM CONTROL CONFIGURATION 123
11 CLASS OF SERVICE 125
Layer 2 Queue Settings 125
Setting the Default Priority for Interfaces 125
Selecting the Queue Mode 126
Mapping CoS Values to Egress Queues 129
Layer 3/4 Priority Settings 132
Setting Priority Processing to DSCP or CoS 132
Mapping Ingress DSCP Values to Internal DSCP Values 133
Mapping CoS Priorities to Internal DSCP Values 136
12 QUALITY OF SERVICE 139
Overview 139
Configuring a Class Map 140
Creating QoS Policies 143
Attaching a Policy Map to a Port 153
13 VOIP TRAFFIC CONFIGURATION 155
Overview 155
Configuring VoIP Traffic 155
Configuring Telephony OUI 157
Configuring VoIP Traffic Ports 158
14 SECURITY MEASURES 161
Configuring Local/Remote Logon Authentication 162
Configuring Remote Logon Authentication Servers 163
Configuring User Accounts 166
Network Access 168
Configuring Global Settings for Network Access 168
Configuring Network Access for Ports 169
Displaying Secure MAC Address Information 170

Configuring HTTPS 172
Configuring Global Settings for HTTPS 172
Replacing the Default Secure-site Certificate 173
Access Control Lists 175
Showing TCAM Utilization 175
Setting the ACL Name and Type 177
Configuring a Standard IPv4 ACL 178
Configuring an Extended IPv4 ACL 179
Configuring a MAC ACL 182
Binding a Port to an Access Control List 184
Filtering IP Addresses for Management Access 185
Configuring Port Security 187
Configuring 802.1X Port Authentication 189
Configuring 802.1X Global Settings 191
Configuring Port Authenticator Settings for 802.1X 192
Configuring Port Supplicant Settings for 802.1X 196
Displaying 802.1X Statistics 198
15 BASIC ADMINISTRATION PROTOCOLS 201
Configuring Event Logging 201
System Log Configuration 201
Remote Log Configuration 204
Link Layer Discovery Protocol 205
Setting LLDP Timing Attributes 206
Configuring LLDP Interface Attributes 208
Configuring LLDP Interface Civic-Address 211
Displaying LLDP Local Device Information 214
Displaying LLDP Remote Port Information 216
Displaying Device Statistics 221
Power over Ethernet 224
Displaying the Switch's Overall PoE Power Budget 225
Setting The Port PoE Power Budget 226
Simple Network Management Protocol 227
Configuring Global Settings for SNMP 230
Setting the Local Engine ID 231
Specifying a Remote Engine ID 232
Setting SNMPv3 Views 233

Configuring SNMPv3 Groups 236
Setting Community Access Strings 240
Configuring Local SNMPv3 Users 241
Configuring Remote SNMPv3 Users 243
Specifying Trap Managers 245
Remote Monitoring 250
Configuring RMON Alarms 250
Configuring RMON Events 253
Configuring RMON History Samples 255
Configuring RMON Statistical Samples 258
Switch Clustering 261
Configuring General Settings for Clusters 261
Cluster Member Configuration 263
Managing Cluster Members 264

16 IP CONFIGURATION 267

Using the Ping Function 267
Address Resolution Protocol 268
Setting the ARP Timeout 269
Displaying ARP Entries 270
Setting the Switch's IP Address (IP Version 4) 271

17 MULTICAST FILTERING 275

Layer 2 IGMP (Snooping and Query) 276
Configuring IGMP Snooping and Query Parameters 277
Specifying Static Interfaces for a Multicast Router 280
Assigning Interfaces to Multicast Services 282
Setting IGMP Snooping Status per Interface 284
Displaying Multicast Groups Discovered by IGMP Snooping 289
Filtering and Throttling IGMP Groups 290
Enabling IGMP Filtering and Throttling 290
Configuring IGMP Filter Profiles 291
Configuring IGMP Filtering and Throttling for Interfaces 293

SECTION III APPENDICES 295

A SOFTWARE SPECIFICATIONS 297

Software Features 297

Management Features 298
Standards 298
Management Information Bases 299
B TROUBLESHOOTING 301
Problems Accessing the Management Interface 301
Using System Logs 302
C LICENSE INFORMATION 303
The GNU General Public License 303
GLOSSARY 307
INDEX 313

FIGURES

Figure 1: Home Page 35
Figure 2: Front Panel Indicators 37
Figure 3: Displaying Configuration Settings or Status Information 38
Figure 4: System Information 48
Figure 5: General Switch Information 49
Figure 6: Configuring Support for Jumbo Frames 50
Figure 7: Displaying Bridge Extension Configuration 52
Figure 8: Copy Firmware 54
Figure 9: Saving the Running Configuration 55
Figure 10: Setting Start-Up Files 56
Figure 11: Displaying System Files 56
Figure 12: Manually Setting the System Clock 58
Figure 13: Setting the Polling Interval for SNTP 59
Figure 14: Specifying SNTP Time Servers 59
Figure 15: Setting the Time Zone 61
Figure 16: Displaying CPU Utilization 62
Figure 17: Displaying Memory Utilization 63
Figure 18: Restarting the Switch 64
Figure 19: Configuring Connections by Port List 67
Figure 20: Configuring Connections by Port Range 68
Figure 21: Displaying Port Information 69
Figure 22: Configuring Local Port Mirroring 69
Figure 23: Configuring Local Port Mirroring 70
Figure 24: Displaying Local Port Mirror Sessions 71
Figure 25: Showing Port Statistics (Table) 74
Figure 26: Showing Port Statistics (Chart) 75
Figure 27: Performing Cable Tests 77
Figure 28: Configuring Static Trunks 78
Figure 29: Creating Static Trunks 79
Figure 30: Configuring Connection Parameters for a Static Trunk 80
Figure 31: Showing Information for Static Trunks 80

Figure 32: Configuring Dynamic Trunks 80
Figure 33: Configuring the LACP Aggregator Admin Key 82
Figure 34: Enabling LACP on a Port 83
Figure 35: Configuring LACP Parameters on a Port 84
Figure 36: Configuring Connection Parameters for a Dynamic Trunk 84
Figure 37: Showing Connection Parameters for Dynamic Trunks 85
Figure 38: Showing Members of Dynamic Trunks 85
Figure 39: Displaying LACP Port Counters 86
Figure 40: Displaying LACP Port Internal Information 88
Figure 41: Displaying LACP Port Remote Information 89
Figure 42: Configuring Trunk Mirroring 89
Figure 43: Configuring Trunk Mirroring 90
Figure 44: Displaying Trunk Mirror Sessions 91
Figure 45: Enabling Power Savings 92
Figure 46: VLAN Compliant and VLAN Non-compliant Devices 94
Figure 47: Creating Static VLANs 96
Figure 48: Configuring Static Members by VLAN Index 98
Figure 49: Configuring Static VLAN Members by Interface 99
Figure 50: Configuring Static VLAN Members by Interface Range 100
Figure 51: Configuring Static MAC Addresses 102
Figure 52: Displaying Static MAC Addresses 102
Figure 53: Setting the Address Aging Time 103
Figure 54: Displaying the Dynamic MAC Address Table 105
Figure 55: Clearing Entries in the Dynamic MAC Address Table 106
Figure 56: STP Root Ports and Designated Ports 108
Figure 57: Configuring Global Settings for STA (STP) 111
Figure 58: Configuring Global Settings for STA (RSTP) 111
Figure 59: Displaying Global Settings for STA 113
Figure 60: Configuring Interface Settings for STA 116
Figure 61: STA Port Roles 117
Figure 62: Displaying Interface Settings for STA 118
Figure 63: Configuring Rate Limits 121
Figure 64: Configuring Storm Control 124
Figure 65: Setting the Default Port Priority 126
Figure 66: Setting the Queue Mode (Strict) 128
Figure 67: Setting the Queue Mode (WRR) 128

Figure 68: Setting the Queue Mode (Strict and WRR) 129
Figure 69: Mapping CoS Values to Egress Queues 131
Figure 70: Showing CoS Values to Egress Queue Mapping 131
Figure 71: Setting the Trust Mode 133
Figure 72: Configuring DSCP to DSCP Internal Mapping 135
Figure 73: Showing DSCP to DSCP Internal Mapping 135
Figure 74: Configuring CoS to DSCP Internal Mapping 137
Figure 75: Showing CoS to DSCP Internal Mapping 138
Figure 76: Configuring a Class Map 141
Figure 77: Showing Class Maps 142
Figure 78: Adding Rules to a Class Map 142
Figure 79: Showing the Rules for a Class Map 143
Figure 80: Configuring a Policy Map 151
Figure 81: Showing Policy Maps 151
Figure 82: Adding Rules to a Policy Map 152
Figure 83: Showing the Rules for a Policy Map 152
Figure 84: Attaching a Policy Map to a Port 153
Figure 85: Configuring a Voice VLAN 156
Figure 86: Configuring an OUI Telephony List 158
Figure 87: Showing an OUI Telephony List 158
Figure 88: Configuring Port Settings for a Voice VLAN 160
Figure 89: Configuring the Authentication Sequence 163
Figure 90: Authentication Server Operation 163
Figure 91: Configuring Remote Authentication Server (RADIUS) 165
Figure 92: Configuring Remote Authentication Server (TACACS+) 166
Figure 93: Configuring User Accounts 167
Figure 94: Showing User Accounts 167
Figure 95: Configuring Global Settings for Network Access 169
Figure 96: Configuring Interface Settings for Network Access 170
Figure 97: Showing Addresses Authenticated for Network Access 171
Figure 98: Configuring HTTPS 173
Figure 99: Downloading the Secure-Site Certificate 175
Figure 100: Showing TCAM Utilization 176
Figure 101: Creating an ACL 177
Figure 102: Showing a List of ACLs 178
Figure 103: Configuring a Standard IPv4 ACL 179

Figure 104: Configuring an Extended IPv4 ACL 181
Figure 105: Configuring a MAC ACL 183
Figure 106: Binding a Port to an ACL 184
Figure 107: Creating an IP Address Filter for Management Access 186
Figure 108: Showing IP Addresses Authorized for Management Access 186
Figure 109: Setting the Maximum Address Count for Port Security 188
Figure 110: Configuring the Status and Response for Port Security 189
Figure 111: Configuring Port Security 190
Figure 112: Configuring Global Settings for 802.1X Port Authentication 192
Figure 113: Configuring Interface Settings for 802.1X Port Authenticator 195
Figure 114: Configuring Interface Settings for 802.1X Port Supplicant 197
Figure 115: Showing Statistics for 802.1X Port Authenticator 199
Figure 116: Showing Statistics for 802.1X Port Supplicant 200
Figure 117: Configuring Settings for System Memory Logs 203
Figure 118: Showing Error Messages Logged to System Memory 203
Figure 119: Configuring Settings for Remote Logging of Error Messages 205
Figure 120: Configuring LLDP Timing Attributes 207
Figure 121: Configuring LLDP Interface Attributes 211
Figure 122: Configuring the Civic Address for an LLDP Interface 213
Figure 123: Showing the Civic Address for an LLDP Interface 213
Figure 124: Displaying Local Device Information for LLDP (General) 215
Figure 125: Displaying Local Device Information for LLDP (Port) 216
Figure 126: Displaying Remote Device Information for LLDP (Port) 220
Figure 127: Displaying Remote Device Information for LLDP (Port Details) 221
Figure 128: Displaying LLDP Device Statistics (General) 223
Figure 129: Displaying LLDP Device Statistics (Port) 223
Figure 130: Showing the Switch’s PoE Budget 225
Figure 131: Setting a Port’s PoE Budget 227
Figure 132: Configuring Global Settings for SNMP 230
Figure 133: Configuring the Local Engine ID for SNMP 231
Figure 134: Configuring a Remote Engine ID for SNMP 232
Figure 135: Showing Remote Engine IDs for SNMP 233
Figure 136: Creating an SNMP View 234
Figure 137: Showing SNMP Views 234
Figure 138: Adding an OID Subtree to an SNMP View 235
Figure 139: Showing the OID Subtree Configured for SNMP Views 235

Figure 140: Creating an SNMP Group 239
Figure 141: Showing SNMP Groups 239
Figure 142: Setting Community Access Strings 240
Figure 143: Showing Community Access Strings 241
Figure 144: Configuring Local SNMPv3 Users 242
Figure 145: Showing Local SNMPv3 Users 243
Figure 146: Configuring Remote SNMPv3 Users 245
Figure 147: Showing Remote SNMPv3 Users 245
Figure 148: Configuring Trap Managers (SNMPv1) 248
Figure 149: Configuring Trap Managers (SNMPv2c) 249
Figure 150: Configuring Trap Managers (SNMPv3) 249
Figure 151: Showing Trap Managers 250
Figure 152: Configuring an RMON Alarm 252
Figure 153: Showing Configured RMON Alarms 253
Figure 154: Configuring an RMON Event 254
Figure 155: Showing Configured RMON Events 255
Figure 156: Configuring an RMON History Sample 256
Figure 157: Showing Configured RMON History Samples 257
Figure 158: Showing Collected RMON History Samples 258
Figure 159: Configuring an RMON Statistical Sample 259
Figure 160: Showing Configured RMON Statistical Samples 260
Figure 161: Showing Collected RMON Statistical Samples 260
Figure 162: Configuring a Switch Cluster 262
Figure 163: Configuring a Cluster Members 263
Figure 164: Showing Cluster Members 264
Figure 165: Showing Cluster Candidates 264
Figure 166: Managing a Cluster Member 265
Figure 167: Pinging a Network Device 268
Figure 168: Setting the ARP Timeout 270
Figure 169: Displaying ARP Entries 270
Figure 170: Configuring a Static IPv4 Address 272
Figure 171: Configuring a Dynamic IPv4 Address 273
Figure 172: Multicast Filtering Concept 275
Figure 173: Configuring General Settings for IGMP Snooping 280
Figure 174: Configuring a Static Interface for a Multicast Router 281
Figure 175: Showing Static Interfaces Attached a Multicast Router 281

Figure 176: Showing Current Interfaces Attached a Multicast Router 282
Figure 177: Assigning an Interface to a Multicast Service 283
Figure 178: Showing Static Interfaces Assigned to a Multicast Service 283
Figure 179: Showing Current Interfaces Assigned to a Multicast Service 284
Figure 180: Configuring IGMP Snooping on an Interface 288
Figure 181: Showing Interface Settings for IGMP Snooping 288
Figure 182: Showing Multicast Groups Learned by IGMP Snooping 289
Figure 183: Enabling IGMP Filtering and Throttling 291
Figure 184: Creating an IGMP Filtering Profile 292
Figure 185: Showing the IGMP Filtering Profiles Created 292
Figure 186: Adding Multicast Groups to an IGMP Filtering Profile 293
Figure 187: Showing the Groups Assigned to an IGMP Filtering Profile 293
Figure 188: Configuring IGMP Filtering and Throttling Interface Settings 294

TABLES

Table 1:	Key Features	23
Table 2:	System Defaults	28
Table 3:	Web Page Configuration Buttons	36
Table 4:	Switch Main Menu	39
Table 5:	Port Statistics	71
Table 6:	LACP Port Counters	85
Table 7:	LACP Internal Configuration Information	87
Table 8:	LACP Internal Configuration Information	88
Table 9:	Recommended STA Path Cost Range	115
Table 10:	Default STA Path Costs	115
Table 11:	Effective Rate Limit	120
Table 12:	IEEE 802.1p Egress Queue Priority Mapping	129
Table 13:	CoS Priority Levels	130
Table 14:	Mapping Internal Per-hop Behavior to Hardware Queues	130
Table 15:	Default Mapping of DSCP Values to Internal PHB/Drop Values	134
Table 16:	Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	137
Table 17:	HTTPS System Support	172
Table 18:	802.1X Statistics	198
Table 19:	Logging Levels	202
Table 20:	LLDP MED Location CA Types	212
Table 21:	Chassis ID Subtype	214
Table 22:	System Capabilities	214
Table 23:	Port ID Subtype	217
Table 24:	Remote Port Auto-Negotiation Advertised Capability	218
Table 25:	SNMPv3 Security Models and Levels	228
Table 26:	Supported Notification Messages	236
Table 27:	Address Resolution Protocol	269
Table 28:	Troubleshooting Chart	301

SECTION I

GETTING STARTED

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- "Introduction" on page 23
- "Initial Switch Configuration" on page 31

1 INTRODUCTION

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

KEY FEATURES

Table 1: Key Features

Feature	Description
Configuration Backup and Restore	Using management station
Authentication	Web – user name/password, RADIUS, TACACS+, HTTPS SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X, MAC address filtering
General Security Measures	Port Authentication Port Security
Access Control Lists	Supports up to 512 rules, 64 ACLs, and a maximum of 32 rules for an ACL
DHCP	Client
Port Configuration	Speed and duplex mode and flow control
Port Trunking	Supports up to 12 trunks – static or dynamic trunking (LACP)
Port Mirroring	24 sessions, one or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms Random Early Detection
Address Table	8K MAC addresses in the forwarding table, 1K static MAC addresses, 256 L2 multicast groups
IP Version 4	Supports IPv4 addressing, and management
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP and Rapid Spanning Tree Protocol (RSTP)
Virtual LANs	Up to 128 using IEEE 802.1Q, port-based
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP)
Qualify of Service	Supports Differentiated Services (DiffServ)

Table 1: Key Features (Continued)

Feature	Description
Link Layer Discovery Protocol	Used to discover basic information about neighboring devices
Multicast Filtering	Supports IGMP snooping and query

DESCRIPTION OF SOFTWARE FEATURES

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Untagged (port-based) and tagged VLANs provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications.

Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

You can save the current configuration settings to a file on the management station (using the web interface), and later download this file to restore the switch configuration settings.

AUTHENTICATION

This switch authenticates management access via a web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication server to verify the client's right to access the network via an authentication server (i.e., RADIUS or TACACS+ server).

Other authentication options include HTTPS for secure management access via the web, SNMP Version 3, IP address filtering for web/SNMP management access, and MAC address filtering for port access.

ACCESS CONTROL LISTS

ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

PORT CONFIGURATION You can manually configure the speed and duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

PORT MIRRORING The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

PORT TRUNKING Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 12 trunks.

RATE LIMITING This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

STORM CONTROL Broadcast, multicast and unknown unicast storm suppression prevents traffic from overwhelming the network.When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

STATIC ADDRESSES A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D BRIDGE

The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 8K addresses.

STORE-AND-FORWARD SWITCHING

The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 1 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

SPANNING TREE ALGORITHM

The switch supports these spanning tree protocols:

- Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

VIRTUAL LANS

The switch supports up to 128 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.

- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.

- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.

TRAFFIC PRIORITIZATION

This switch prioritizes each packet based on the required level of service, using four priority queues with strict priority, Weighted Round Robin (WRR) scheduling, or a combination of strict and weighted queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet using DSCP, or IP Precedence. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

QUALITY OF SERVICE

Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

MULTICAST FILTERING

Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

SYSTEM DEFAULTS

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file.

The following table lists some of the basic system defaults.

Table 2: System Defaults

Function	Parameter	Default
Authentication	RADIUS Authentication	Disabled
	TACACS+ Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Disabled Multicast: Disabled Unknown Unicast: Disabled
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Disabled
LLDP	Status	Enabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Access
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	Strict-WRR
	Queue Weight	Queue: 0 1 2 3 Weight: 1 2 4 6
	Class of Service	Enabled
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
IP Settings	Management VLAN	VLAN 1
	IP Address	192.168.1.10
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled
	BOOTP	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Disabled Querier: Disabled
System Log	Status	Enabled
	Messages Logged to RAM	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SNTP	Clock Synchronization	Disabled

2 INITIAL SWITCH CONFIGURATION

This chapter includes information on connecting to the switch and basic configuration procedures.

To make use of the management features of your switch, you must first configure it with an IP address that is compatible with the network in which it is being installed. This should be done before you permanently install the switch in the network.

Follow this procedure:

1. Place the switch close to the PC that you intend to use for configuration. It helps if you can see the front panel of the switch while working on your PC.

2. Connect the Ethernet port of your PC to any port on the front panel of the switch. Connect power to the switch and verify that you have a link by checking the front-panel LEDs.

3. Check that your PC has an IP address on the same subnet as the switch. The default IP address of the switch is 192.168.1.10 and the subnet mask is 255.255.255.0, so the PC and switch are on the same subnet if they both have addresses that start 192.168.1.x. If the PC and switch are not on the same subnet, you must manually set the PC's IP address to 192.168.1.x (where "x" is any number from 1 to 255, except 10).

4. Open your web browser and enter the address http://192.168.1.10. If your PC is properly configured, you will see the login page of the switch. If you do not see the login page, repeat step 3.

5. Enter "admin" for the user name and password, and then click on the Login button.

6. From the menu, click on System, and then click on IP. Enter the new IP address, Subnet Mask and Gateway IP Address for the switch, and then click on the Apply button.

No other configuration changes are required at this stage, but it is recommended that you change the administrator's password before logging out. To change the password, click Security and then User Accounts. Select Modify from the Action list. Select "admin" from the User Name list, fill in the Password, and then click Apply.

SECTION II

WEB CONFIGURATION

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser.

This section includes these chapters:

- "Using the Web Interface" on page 35
- "Basic Management Tasks" on page 47
- "Interface Configuration" on page 65
- "VLAN Configuration" on page 93
- "Address Table Settings" on page 101
- "Spanning Tree Algorithm" on page 107
- "Rate Limit Configuration" on page 119
- "Storm Control Configuration" on page 123
- "Class of Service" on page 125
- "Quality of Service" on page 139
- "VoIP Traffic Configuration" on page 155
- "Security Measures" on page 161
- "Basic Administration Protocols" on page 201
- "IP Configuration" on page 267
- "Multicast Filtering" on page 275

3 USING THE WEB INTERFACE

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above).

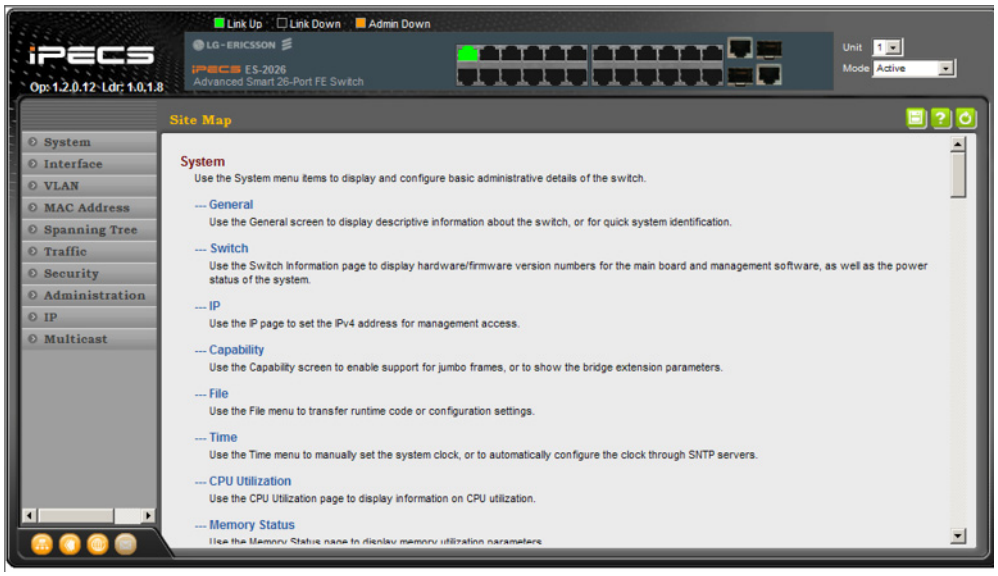
NAVIGATING THE WEB BROWSER INTERFACE

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

HOME PAGE

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Home Page


Link Up
Link Down
Admin Down
iPECS
Op: 1.2.0.12 Ldr: 1.0.1.8
LG-ERICSSON
iPECS ES-2026
Advanced Smart 26-Port FE Switch
Unit 1
Mode Active
Site Map
System
Interface
VLAN
MAC Address
Spanning Tree
Traffic
Security
Administration
IP
Multicast
System
Use the System menu items to display and configure basic administrative details of the switch.
General
Use the General screen to display descriptive information about the switch, or for quick system identification.
Switch
Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.
IP
Use the IP page to set the IPv4 address for management access.
Capability
Use the Capability screen to enable support for jumbo frames, or to show the bridge extension parameters.
File
Use the File menu to transfer runtime code or configuration settings.
Time
Use the Time menu to manually set the system clock, or to automatically configure the clock through SNTP servers.
CPU Utilization
Use the CPU Utilization page to display information on CPU utilization.
Memory Status

NOTE: This manual covers the ES-2026 and ES-2026P Fast Ethernet switches, and the ES-2024G and ES-2024GP Gigabit Ethernet switches. Other than the difference in port types supported by the Fast Ethernet and Gigabit Ethernet switches, and support for PoE (ES-2026P, ES-2024GP), there are no other significant differences. Therefore nearly all of the screen display examples are based on the ES-2026. The panel graphics for all of switch types are shown on the following page.

CONFIGURATION OPTIONS

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

Table 3: Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
	Save current configuration settings.
	Displays help for the selected page.
	Refreshes the current page.
	Displays the site map.
	Logs out of the management interface.
	Links to the manufacture's web site.
	Sends mail to the manufacturer.

NOTE: To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

NOTE: When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

PANEL DISPLAY

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control).

Figure 2: Front Panel Indicators

ES-2026



ES-2026P



ES-2024G



ES-2024GP

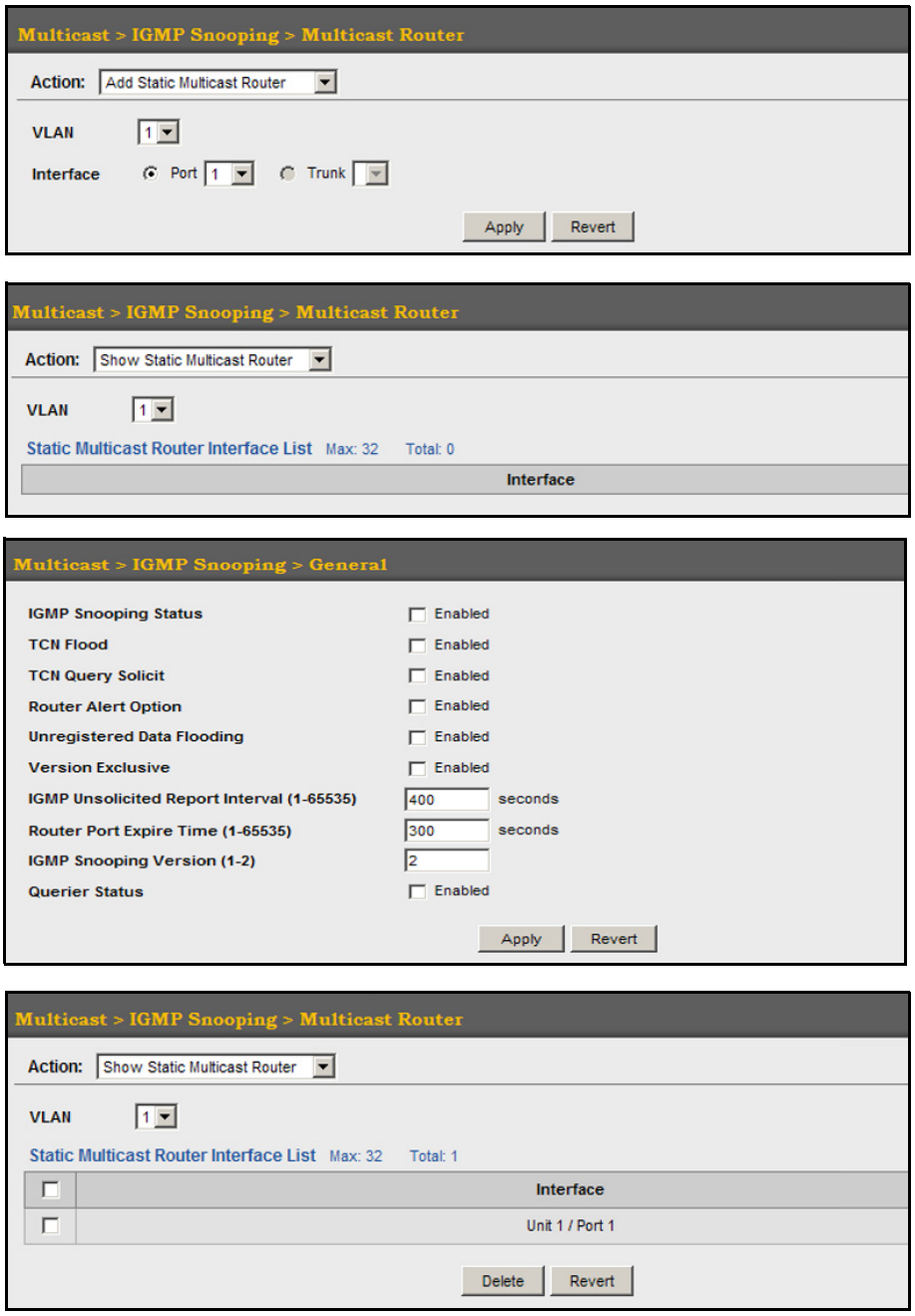


SHOWING STATUS INFORMATION

There are various web pages which display configuration settings or the status of specified processes. Many of these pages will not display any information unless the switch is properly configured, and in some cases the interface to which a command applies is up.

For example, if a static router port is configured, the corresponding information page will not display any information unless IGMP snooping is first enabled, and the link for the static router port is up.

Figure 3: Displaying Configuration Settings or Status Information


Multicast > IGMP Snooping > Multicast Router
Action: Add Static Multicast Router
VLAN 1
Interface Port 1 Trunk
Apply Revert
Multicast > IGMP Snooping > Multicast Router
Action: Show Static Multicast Router
VLAN 1
Static Multicast Router Interface List Max: 32 Total: 0
Interface
Multicast > IGMP Snooping > General
IGMP Snooping Status Enabled
TCN Flood Enabled
TCN Query Solicit Enabled
Router Alert Option Enabled
Unregistered Data Flooding Enabled
Version Exclusive Enabled
IGMP Unsolicited Report Interval (1-65535) 400 seconds
Router Port Expire Time (1-65535) 300 seconds
IGMP Snooping Version (1-2) 2
Querier Status Enabled
Apply Revert
Multicast > IGMP Snooping > Multicast Router
Action: Show Static Multicast Router
VLAN 1
Static Multicast Router Interface List Max: 32 Total: 1
Interface
Unit 1 / Port 1
Delete Revert

MAIN MENU

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 4: Switch Main Menu

Menu	Description	Page
System		
General	Provides basic system description, including contact information	47
Switch	Shows the number of ports, hardware version, power status, and firmware version numbers	48
IP	Sets the IPv4 address for management access	271
Capability	Enables support for jumbo frames; shows the bridge extension parameters	50, 51
File		52
Copy	Allows the transfer and copying files	52
Set Startup	Sets the startup file	55
Show	Shows the files stored in flash memory; allows deletion of files	56
Time		57
Configure General		
Manual	Manually sets the current time	57
SNTP	Configures SNTP polling interval	58
Configure Time Server	Configures a list of SNTP servers	59
Configure Time Zone	Sets the local time zone for the system clock	60
CPU Utilization	Displays information on CPU utilization;	61
Memory Status	Shows memory utilization parameters	62
Reset	Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval	62
Interface		65
Port		65
General		
Configure by Port List	Configures connection settings per port	65
Configure by Port Range	Configures connection settings for a range of ports	68
Show Information	Displays port connection status	68
Mirror		69
Show	Shows the configured mirror sessions	69
Add	Sets the source and target ports for mirroring	69
Statistics	Shows Interface, Etherlike, and RMON port statistics	71
Chart	Shows Interface, Etherlike, and RMON port statistics	71
Cable Test	Performs cable diagnostics for selected port to diagnose any cable faults (short, open etc.) and report the cable length	75

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Trunk		
Static		78
Configure Trunk	Creates a trunk, specifying port members	78
Configure General		78
Show Information	Displays trunk connection settings	78
Configure	Configures trunk connection settings	78
Dynamic		80
Configure Aggregator	Configures administration key for specific LACP groups	80
Configure Aggregation Port		78
Configure		78
General	Allows ports to dynamically join trunks	80
Actor	Configures parameters for link aggregation group members on the local side	80
Partner	Configures parameters for link aggregation group members on the remote side	80
Show Information		
Counters	Displays statistics for LACP protocol messages	85
Internal	Displays configuration settings and operational state for the local side of a link aggregation	87
Neighbors	Displays configuration settings and operational state for the remote side of a link aggregation	88
Configure Trunk		80
Show	Displays trunk connection settings	80
Configure	Configures trunk connection settings	80
Show Member	Show port members of dynamic trunks	80
Mirror		89
Add	Sets the source trunks and target port for mirroring	89
Show	Shows the configured mirror sessions	89
Statistics	Shows Interface, Etherlike, and RMON port statistics	71
Chart	Shows Interface, Etherlike, and RMON port statistics	71
Green Ethernet	Adjusts the power provided to ports based on the length of the cable used to connect to other devices	91
VLAN	Virtual LAN	93
Static		
Configure VLAN	Configures VLAN groups, administrative status, and remote type	95
Modify VLAN and Member Ports	Configures group name, status, and member attributes	96
Edit Member by Interface	Specifies VLAN attributes per interface	96
Edit Member by Interface Range	Specifies VLAN attributes per interface range	96

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
MAC Address		101
Static		101
Add	Configures static entries in the address table	101
Show	Displays static entries in the address table	101
Dynamic		
Configure Aging	Sets timeout for dynamically learned entries	103
Show Dynamic MAC	Displays dynamic entries in the address table	104
Clear Dynamic MAC	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries	105
Spanning Tree		107
STA	Spanning Tree Algorithm	
Configure Global		
Configure	Configures global bridge settings for STP and RSTP	108
Show Information	Displays STA values used for the bridge	112
Configure Interface		
Configure	Configures interface settings for STA	113
Show Information	Displays interface settings for STA	116
Traffic		
Rate Limit	Sets the input and output rate limits for a port	119
Storm Control	Sets the broadcast storm threshold for each interface	123
Priority		
Default Priority	Sets the default priority for each port or trunk	125
Queue	Sets queue mode for the switch; sets the service weight for each queue that will use a weighted or hybrid mode	126
Trust Mode	Selects IP Precedence, DSCP or CoS priority processing	132
DSCP to DSCP		133
Add	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	133
Show	Shows the DSCP to DSCP mapping list	133
CoS to DSCP		136
Add	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing	136
Show	Shows the CoS to DSCP mapping list	136
PHB to Queue		129
Add	Maps internal per-hop behavior values to hardware queues	129
Show	Shows the PHB to Queue mapping list	129

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
DiffServ		139
Configure Class		140
Add	Creates a class map for a type of traffic	140
Show	Shows configured class maps	140
Modify	Modifies the name of a class map	140
Add Rule	Configures the criteria used to classify ingress traffic	140
Show Rule	Shows the traffic classification rules for a class map	140
Configure Policy		143
Add	Creates a policy map to apply to multiple interfaces	143
Show	Shows configured policy maps	143
Modify	Modifies the name of a policy map	143
Add Rule	Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic	143
Show Rule	Shows the rules used to enforce bandwidth policing for a policy map	143
Configure Interface	Applies a policy map to an ingress port	153
VoIP	Voice over IP	155
Configure Global	Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time	155
Configure OUI		157
Add	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	157
Show	Shows the OUI telephony list	157
Configure Interface	Configures VoIP traffic settings for ports, including the way in which a port is added to the Voice VLAN, filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to the voice traffic	158
Security		161
AAA	Authentication, Authorization and Accounting	
System Authentication	Configures authentication sequence – local, RADIUS, and TACACS	162
Server	Configures RADIUS and TACACS server message exchange settings	163
User Accounts		166
Add	Configures user names, passwords, and access levels	166
Show	Shows authorized users	166
Modify	Modifies user attributes	166
Network Access	MAC address-based network access authentication	168
Configure Global	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	168
Configure Interface	Enables dynamic VLAN assignment	169
Show Information	Shows the authenticated MAC address list	170

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
HTTPS	Secure HTTP	172
Configure Global	Enables HTTPs, and specifies the UDP port to use	172
Copy Certificate	Replaces the default secure-site certificate	173
ACL	Access Control Lists	175
Configure ACL		177
Show TCAM	Shows utilization parameters for TCAM	175
Add	Adds an ACL based on IP or MAC address filtering	177
Show	Shows the name and type of configured ACLs	177
Add Rule	Configures packet filtering based on IP or MAC addresses and other packet attributes	177
Show Rule	Shows the rules specified for an ACL	177
Configure Interface	Binds a port to the specified ACL	184
IP Filter		185
Add	Sets IP addresses of clients allowed management access via the web and SNMP	185
Show	Shows the addresses to be allowed management access	185
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	187
Port Authentication	IEEE 802.1X	189
Configure Global	Enables authentication and EAPOL pass-through	191
Configure Interface	Sets authentication parameters for individual ports	192
Authenticator	Sets port authenticator settings	192
Supplicant	Sets port supplicant settings	196
Show Statistics	Displays protocol statistics for the selected port	198
Authenticator	Displays protocol statistics for port authenticator	198
Supplicant	Displays protocol statistics for port supplicant	198
Administration		201
Log		201
System		201
Configure Global	Stores error messages in local memory	201
Show Logs	Shows logged error messages	201
Remote	Configures the logging of messages to a remote logging process	204
LLDP		205
Configure Global	Configures global LLDP timing parameters	206
Configure Interface	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise	208
Configure General	Sets the message transmission mode, enables SNMP notification, and sets the LLDP attributes to advertise	208
Add CA-Type	Specifies the location of the device attached to an interface	211

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Show CA-Type	Shows the location of the device attached to an interface	211
Modify CA-Type	Modifies the location of the device attached to an interface	211
Show Local Device Information		214
General	Displays general information about the local device	214
Port/Trunk	Displays information about each interface	214
Show Remote Device Information		216
Port/Trunk	Displays information about a remote device connected to a port on this switch	216
Port/Trunk Details	Displays detailed information about a remote device connected to this switch	216
Show Device Statistics		221
General	Displays statistics for all connected remote devices	221
Port/Trunk	Displays statistics for remote devices on a selected port or trunk	221
PoE	Power over Ethernet	224
Configure Global	Displays the power budget for the switch	225
Configure Interface	Configures port power parameters	226
SNMP	Simple Network Management Protocol	227
Configure Global	Enables SNMP agent status, and sets related trap functions	230
Configure Engine		231
Set Engine ID	Sets the SNMP v3 engine ID on this switch	231
Add Remote Engine	Sets the SNMP v3 engine ID for a remote device	232
Show Remote Engine	Shows configured engine ID for remote devices	232
Configure View		233
Add View	Adds an SNMP v3 view of the OID MIB	233
Show View	Shows configured SNMP v3 views	233
Add OID Subtree	Specifies a part of the subtree for the selected view	233
Show OID Subtree	Shows the subtrees assigned to each view	233
Configure Group		236
Add	Adds a group with access policies for assigned users	236
Show	Shows configured groups and access policies	236
Configure User		
Add Community	Configures community strings and access mode	240
Show Community	Shows community strings and access mode	240
Add SNMPv3 Local User	Configures SNMPv3 users on this switch	241
Show SNMPv3 Local User	Shows SNMPv3 users configured on this switch	241
Change SNMPv3 Local User Group	Assign a local user to a new group	241
Add SNMPv3 Remote User	Configures SNMPv3 users from a remote device	243

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Show SNMPv3 Remote User	Shows SNMPv3 users set from a remote device	241
Configure Trap		245
Add	Configures trap managers to receive messages on key events that occur this switch	245
Show	Shows configured trap managers	245
RMON	Remote Monitoring	250
Configure Global		
Add		
Alarm	Sets threshold bounds for a monitored variable	250
Event	Creates a response event for an alarm	253
Show		
Alarm	Shows all configured alarms	250
Event	Shows all configured events	253
Configure Interface		
Add		
History	Periodically samples statistics on a physical interface	255
Statistics	Enables collection of statistics on a physical interface	258
Show		
History	Shows sampling parameters for each entry in the history group	255
Statistics	Shows sampling parameters for each entry in the statistics group	258
Show Details		
History	Shows sampled data for each entry in the history group	255
Statistics	Shows sampled data for each entry in the history group	258
Cluster		261
Configure Global	Globally enables clustering for the switch; sets Commander status	261
Configure Member		
Add	Adds switch Members to the cluster	263
Show Candidate	Shows cluster candidates	263
Show Member	Shows cluster switch member; managed switch members	264
IP		267
General		
Ping	Sends ICMP echo request packets to another node on the network	267
ARP	Address Resolution Protocol	268
Configure General	Sets the aging time for dynamic entries in the ARP cache	269
Show Information	Shows entries in the Address Resolution Protocol (ARP) cache	270

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Multicast		275
IGMP Snooping		276
General	Enables multicast filtering; configures parameters for multicast snooping	277
Multicast Router		280
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	280
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	280
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	280
IGMP Member		282
Add Static Member	Statically assigns multicast addresses to the selected VLAN	282
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	282
Show Current Member	Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration	282
Interface		284
Configure	Configures IGMP snooping per VLAN interface	284
Show	Shows IGMP snooping settings per VLAN interface	284
Forwarding Entry	Displays the current multicast groups learned through IGMP Snooping	289
Filter		290
Configure General	Enables IGMP filtering for the switch	290
Configure Profile		291
Add	Adds IGMP filter profile; and sets access mode	291
Show	Shows configured IGMP filter profiles	291
Add Multicast Group Range	Assigns multicast groups to selected profile	291
Show Multicast Group Range	Shows multicast groups assigned to a profile	291
Configure Interface	Assigns IGMP filter profiles to port interfaces and sets throttling action	293

4 BASIC MANAGEMENT TASKS

This chapter describes the following topics:

- Displaying System Information – Provides basic system description, including contact information.
- Displaying Switch Hardware/Software Versions – Shows the hardware version, power status, and firmware versions
- Configuring Support for Jumbo Frames – Enables support for jumbo frames.
- Displaying Bridge Extension Capabilities – Shows the bridge extension parameters.
- Managing System Files – Describes how to upgrade operating software or configuration files, and set the system start-up files.
- Setting the System Clock – Sets the current time manually or through specified SNTP servers.
- Displaying CPU Utilization – Displays information on CPU utilization.
- Displaying Memory Utilization – Shows memory utilization parameters.
- Resetting the System – Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

DISPLAYING SYSTEM INFORMATION

Use the System > General page to identify the system by displaying information such as the device name, location and contact information.

PARAMETERS

These parameters are displayed:

- **System Description** – Brief description of device type.
- **System Object ID** – MIB II object ID for switch's network management subsystem.
  (ES-2024GP: 1.3.6.1.4.1.572.17389.105,
  ES-2024G: 1.3.6.1.4.1.572.17389.106,
  ES-2026P: 1.3.6.1.4.1.572.17389.107,
  ES-2026: 1.3.6.1.4.1.572.17389.108)

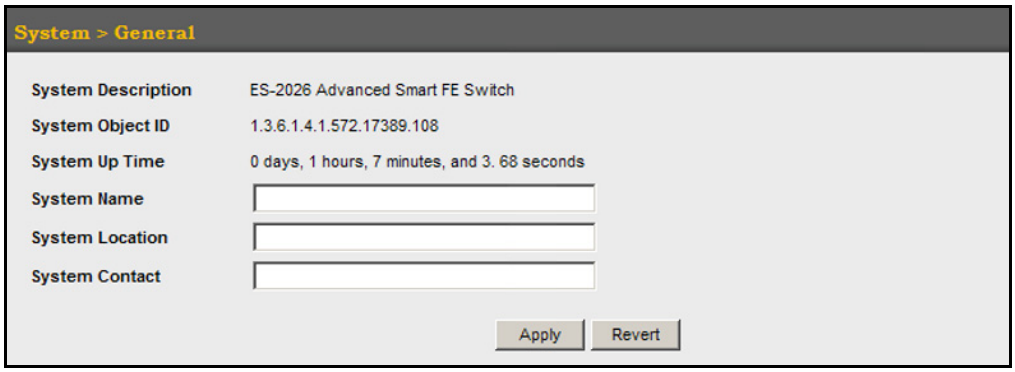
- **System Up Time** – Length of time the management agent has been up.
- **System Name** – Name assigned to the switch system.
- **System Location** – Specifies the system location.
- **System Contact** – Administrator responsible for the system.

WEB INTERFACE

To configure general system information:

1. Click System, General.
2. Specify the system name, location, and contact information for the system administrator.
3. Click Apply.

Figure 4: System Information



DISPLAYING SWITCH HARDWARE/SOFTWARE VERSIONS

Use the System > Switch page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

PARAMETERS

The following parameters are displayed:

Main Board Information

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.

- **Internal Power Status** – Displays the status of the internal power supply.

Management Software Information

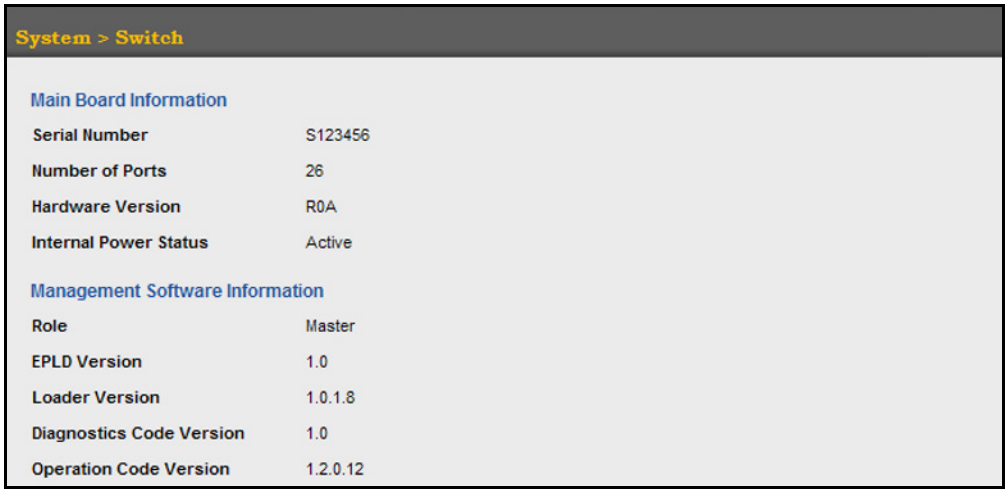
- **Role** – Shows that this switch is operating as Master or Slave.
- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Diagnostics Code Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.

WEB INTERFACE

To view hardware and software version information.

1. Click System, then Switch.

Figure 5: General Switch Information



CONFIGURING SUPPORT FOR JUMBO FRAMES

Use the System > Capability page to configure support for jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes for Gigabit Ethernet. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

USAGE GUIDELINES

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

PARAMETERS

The following parameters are displayed:

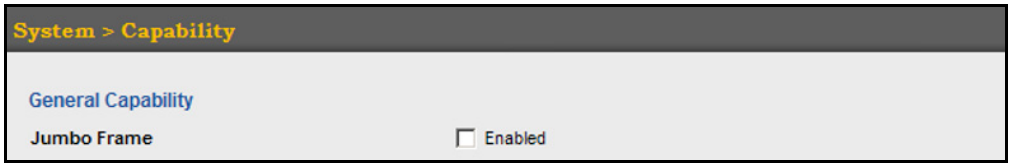
- **Jumbo Frame** – Configures support for jumbo frames. (Default: Disabled)

WEB INTERFACE

To configure support for jumbo frames:

1. Click System, then Capability.
2. Enable or disable support for jumbo frames.
3. Click Apply.

Figure 6: Configuring Support for Jumbo Frames



DISPLAYING BRIDGE EXTENSION CAPABILITIES

Use the System > Capability page to display settings based on the Bridge MIB. The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

PARAMETERS

The following parameters are displayed:

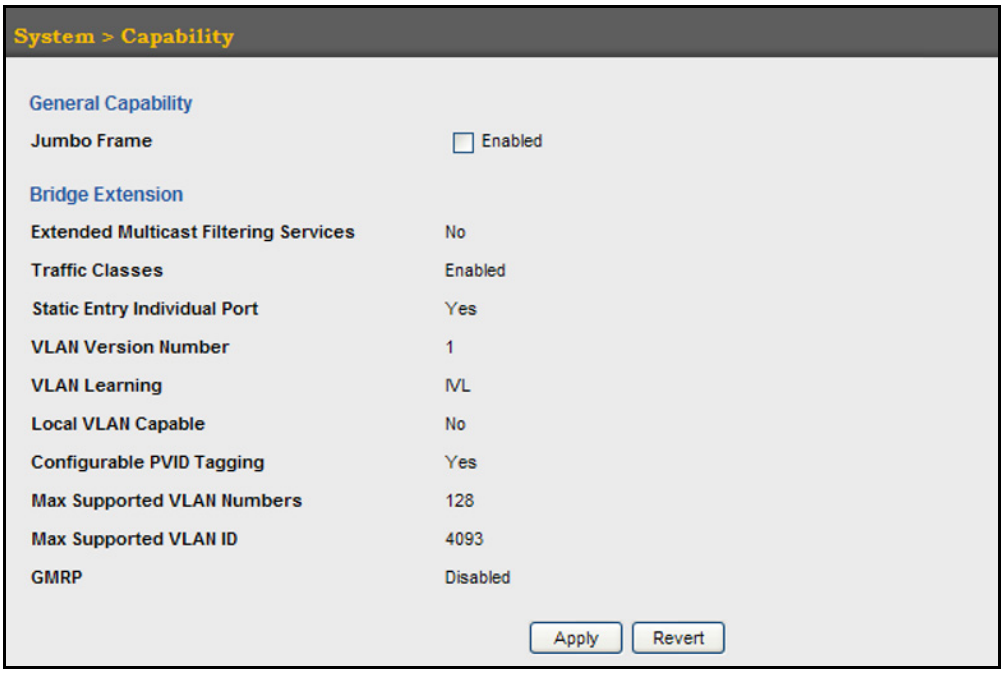
- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service" on page 125.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 101.)
- **VLAN Version Number** – Based on IEEE 802.1Q, "1" indicates Bridges that support only single spanning tree (SST) operation, and "2" indicates Bridges that support multiple spanning tree (MST) operation.
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 93.)
- **Max Supported VLAN Numbers** – The maximum number of VLANs supported on this switch.
- **Max Supported VLAN ID** – The maximum configurable VLAN identifier supported on this switch.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

WEB INTERFACE

To view Bridge Extension information:

1. Click System, then Capability.

Figure 7: Displaying Bridge Extension Configuration



MANAGING SYSTEM FILES

This section describes how to upgrade the switch operating software or configuration files, and set the system start-up files.

COPYING FILES VIA HTTP

Use the System > File (Copy) page to upload/download firmware or configuration settings using HTTP. By backing up a file to a management station, that file can later be downloaded to the switch to restore operation. Specify the file type and file names as required.

You can also set the switch to use new firmware or configuration settings without overwriting the current version. Just download the file using a different name from the current version, and then set the new file as the startup file.

PARAMETERS

The following parameters are displayed:

- **Copy Type** – The firmware copy operation includes these options:
  - HTTP Upgrade – Copies a file from a management station to the switch.

  - HTTP Download – Copies a file from the switch to a management station

- **File Type** – Specify Operation Code, Config File, or Loader.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

NOTE: Only one copy of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch.

NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

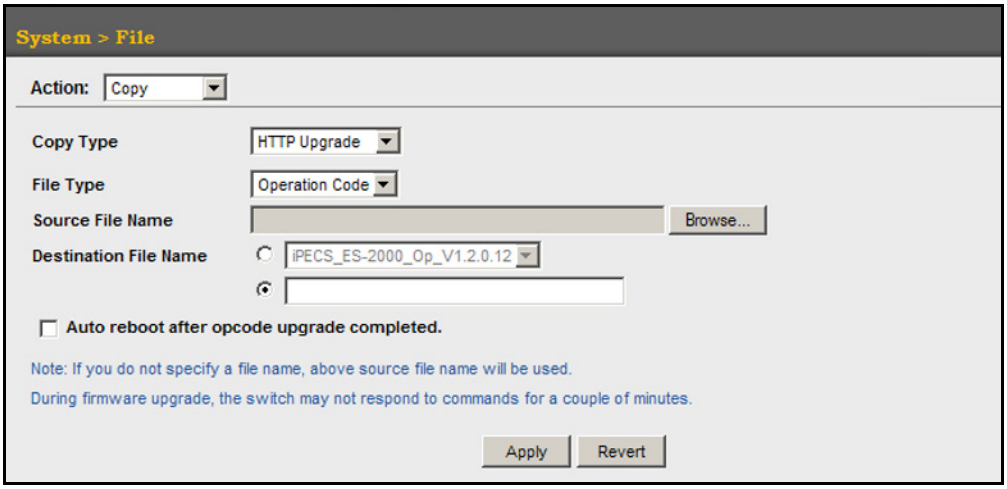
NOTE: The file "Factory_Default_Config.cfg" can be copied to a management station, but cannot be used as the destination file name on the switch.

WEB INTERFACE

To copy firmware files:

1. Click System, then File.
2. Select Copy from the Action list.
3. Select HTTP Upgrade as the file transfer method.
4. Set the file type to Operation Code, Config File, or Loader.
5. Enter the name of the file to download.
6. Select a file on the switch to overwrite or specify a new file name.
7. Then click Apply.

Figure 8: Copy Firmware


System > File
Action: Copy
Copy Type
HTTP Upgrade
File Type
Operation Code
Source File Name
Browse...
Destination File Name
iPECS_ES-2000_Op_V1.2.0.12
Auto reboot after opcode upgrade completed.
Note: If you do not specify a file name, above source file name will be used.
During firmware upgrade, the switch may not respond to commands for a couple of minutes.
Apply
Revert

If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SAVING THE RUNNING CONFIGURATION TO A LOCAL FILE

Use the System > File (Copy) page to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

PARAMETERS

The following parameters are displayed:

- **Copy Type** – The copy operation includes this option:
  - Running-Config – Copies the current configuration settings to a local file on the switch.
- **Destination File Name** – Copy to the currently designated startup file, or to a new file. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

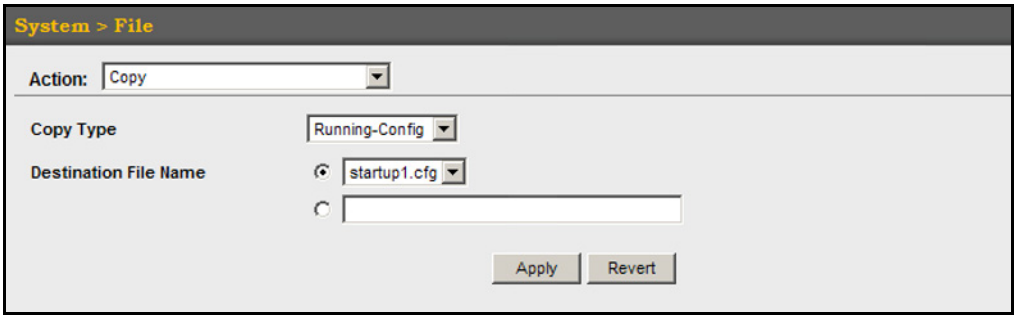
NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

WEB INTERFACE

To save the running configuration file:

1. Click System, then File.
2. Select Copy from the Action list.
3. Select Running-Config from the Copy Type list.
4. Select the current startup file on the switch to overwrite or specify a new file name.
5. Then click Apply.

Figure 9: Saving the Running Configuration



If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SETTING THE START-UP FILE

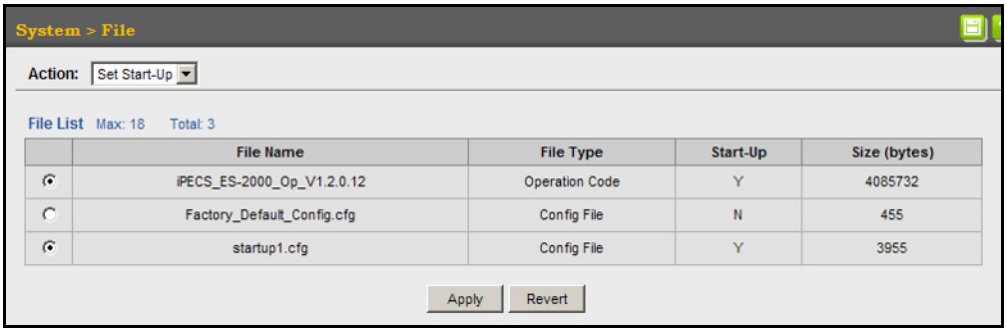
Use the System > File (Set Start-Up) page to specify the firmware or configuration file to use for system initialization.

WEB INTERFACE

To set a file to use for system initialization:

1. Click System, then File.
2. Select Set Start-Up from the Action list.
3. Mark the operation code or configuration file to be used at startup
4. Then click Apply.

Figure 10: Setting Start-Up Files



To start using the new firmware or configuration settings, reboot the system via the System > Reset menu.

SHOWING SYSTEM FILES

Use the System > File (Show) page to show the files in the system directory, or to delete a file.

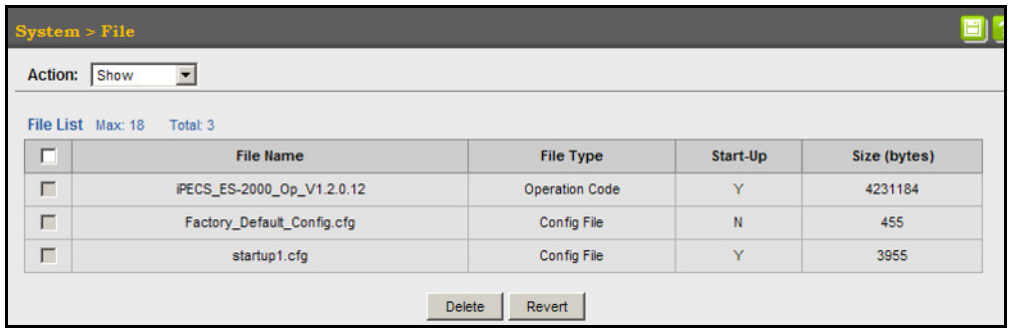
NOTE: Files designated for start-up, and the Factory_Default_Config.cfg file, cannot be deleted.

WEB INTERFACE

To show the system files:

1. Click System, then File.
2. Select Show from the Action list.
3. To delete a file, mark it in the File List and click Delete.

Figure 11: Displaying System Files



SETTING THE SYSTEM CLOCK

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

SETTING THE TIME MANUALLY

Use the System > Time (Configure General - Manually) page to set the system time on the switch manually without using SNTP.

PARAMETERS

The following parameters are displayed:

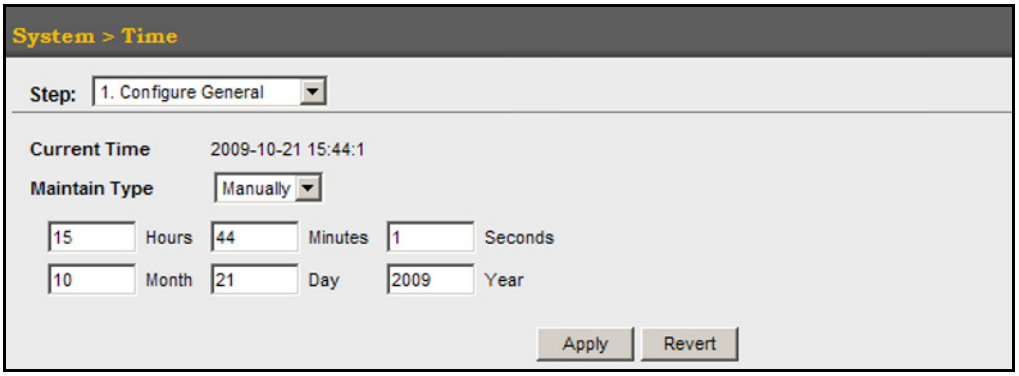
- **Current Time** – Shows the current time set on the switch.
- **Hours** – Sets the hour. (Range: 0-23; Default: 0)
- **Minutes** – Sets the minute value. (Range: 0-59; Default: 0)
- **Seconds** – Sets the second value. (Range: 0-59; Default: 0)
- **Month** – Sets the month. (Range: 1-12; Default: 1)
- **Day** – Sets the day of the month. (Range: 1-31; Default: 1)
- **Year** – Sets the year. (Range: 2001-2100; Default: 2009)

WEB INTERFACE

To manually set the system clock:

1. Click System, then Time.
2. Select Configure General from the Action list.
3. Select Manually from the Maintain Type list.
4. Enter the time and date in the appropriate fields.
5. Click Apply

Figure 12: Manually Setting the System Clock



SETTING THE SNTP POLLING INTERVAL

Use the System > Time (Configure General - SNTP) page to set the polling interval at which the switch will query the specified time servers.

PARAMETERS

The following parameters are displayed:

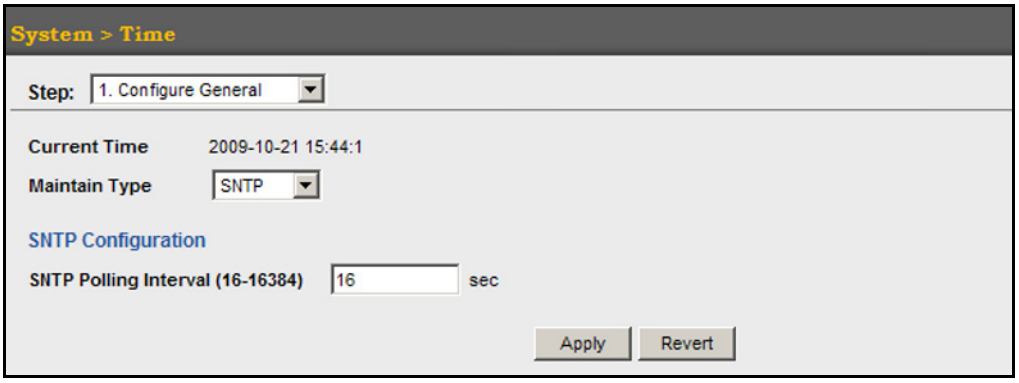
- **Current Time** – Shows the current time set on the switch.
- **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

WEB INTERFACE

To set the polling interval for SNTP:

1. Click System, then Time.
2. Select Configure General from the Action list.
3. Select SNTP from the Maintain Type list.
4. Modify the polling interval if required.
5. Click Apply

Figure 13: Setting the Polling Interval for SNTP



SPECIFYING SNTP TIME SERVERS

Use the System > Time (Configure Time Server) page to specify the IP address for up to three SNTP time servers.

PARAMETERS

The following parameters are displayed:

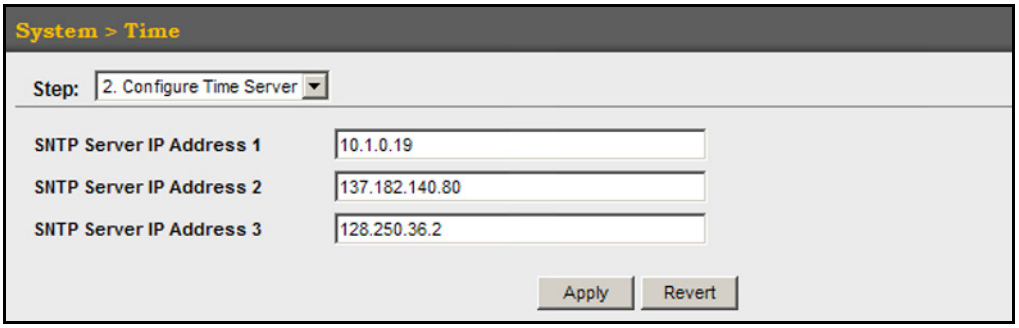
- **SNTP Server IP Address** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

WEB INTERFACE

To set the SNTP time servers:

1. Click System, then Time.
2. Select Configure Time Server from the Action list.
3. Enter the IP address of up to three time servers.
4. Click Apply.

Figure 14: Specifying SNTP Time Servers


System > Time
Step: 2. Configure Time Server
SNTP Server IP Address 1 10.1.0.19
SNTP Server IP Address 2 137.182.140.80
SNTP Server IP Address 3 128.250.36.2
Apply
Revert

SETTING THE TIME ZONE

Use the System > Time (Configure Time Server) page to set the time zone. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude, which passes through Greenwich, England. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC. You can choose one of the 80 predefined time zone definitions, or your can manually configure the parameters for your local time zone.

PARAMETERS

The following parameters are displayed:

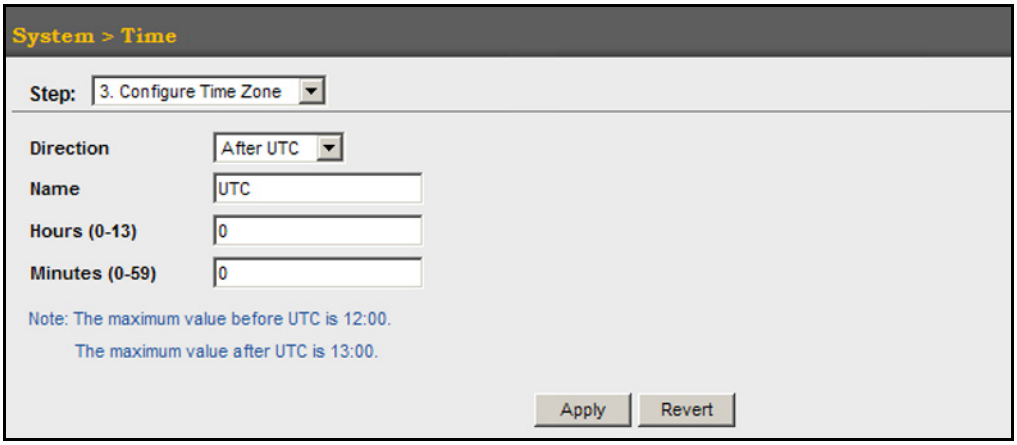
- **Predefined Configuration** – A drop-down box provides access to the 80 predefined time zone configurations. Each choice indicates it's offset from UTC and lists at least one major city or location covered by the time zone.
- **User-defined Configuration** – Allows the user to define all parameters of the local time zone.
  - **Direction**: Configures the time zone to be before (east of) or after (west of) UTC.
  - **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
  - **Hours** (0-13) – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
  - **Minutes** (0-59) – The number of minutes before/after UTC.

WEB INTERFACE

To set your local time zone:

1. Click System, then Time.
2. Select Configure Time Zone from the Action list.
3. Set the offset for your time zone relative to the UTC in hours and minutes using either a predefined or custom definition.
4. Click Apply.

Figure 15: Setting the Time Zone



DISPLAYING CPU UTILIZATION

Use the System > CPU Utilization page to display information on CPU utilization.

PARAMETERS

The following parameters are displayed:

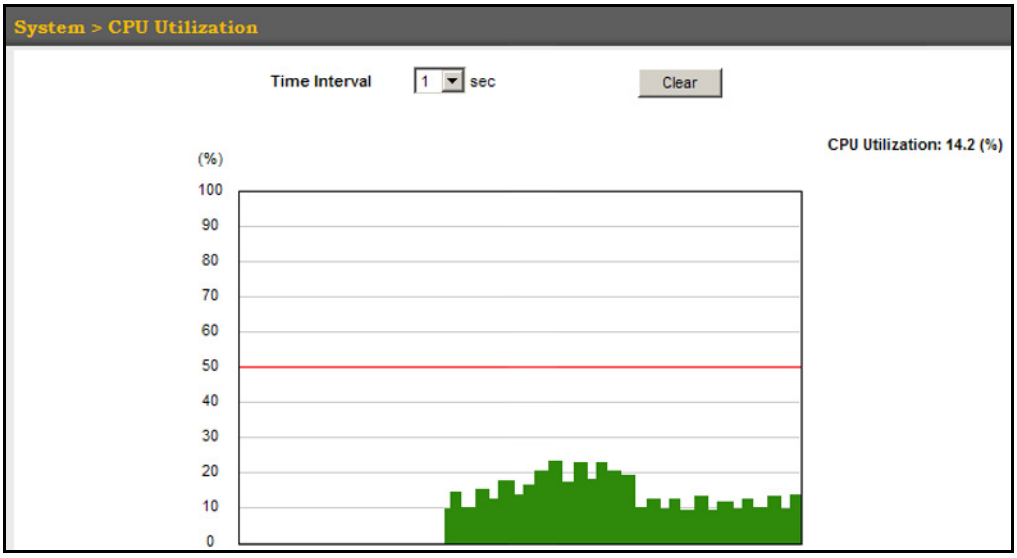
- **Time Interval** – The interval at which to update the displayed utilization rate. (Options: 1, 5, 10, 30, 60 seconds; Default: 1 second)
- **CPU Utilization** – CPU utilization over specified interval.

WEB INTERFACE

To display CPU utilization:

1. Click System, then CPU Utilization.
2. Change the update interval if required. Note that the interval is changed as soon as a new setting is selected.

Figure 16: Displaying CPU Utilization



DISPLAYING MEMORY UTILIZATION

Use the System > Memory Status page to display memory utilization parameters.

PARAMETERS

The following parameters are displayed:

- **Free Size** – The amount of memory currently free for use.
- **Used Size** – The amount of memory allocated to active processes.
- **Total** – The total amount of system memory.

WEB INTERFACE

To display memory utilization:

1. Click System, then Memory Status.

Figure 17: Displaying Memory Utilization



RESETTING THE SYSTEM

Use the System > Reset menu to restart the switch immediately.

COMMAND USAGE

- This command resets the entire system.
- To retain all configuration information stored in non-volatile memory, click the Save button prior to resetting the system.
- When the system is restarted, it will always run the Power-On Self-Test.

PARAMETERS

The following parameters are displayed:

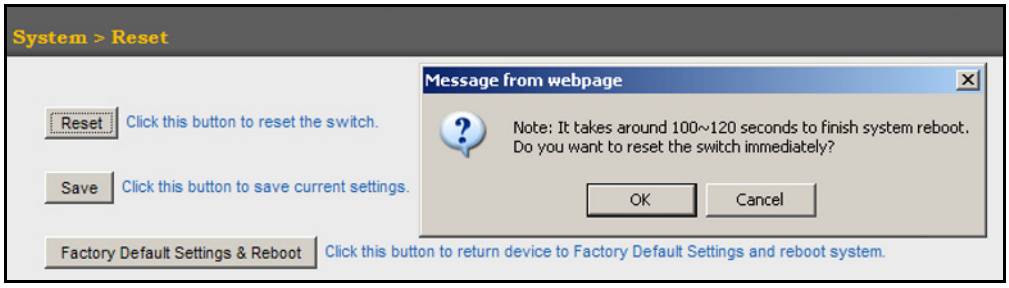
- **Reset** – Restarts the switch immediately.
- **Save** – Click this button to save the current configuration settings.
- **Factory Default Settings & Reboot** – Click this button to restore the factory default settings and reboot the system.

WEB INTERFACE

To restart the switch:

1. Click System, then Reset.
2. Click the Reset button.
3. When prompted, confirm that you want reset the switch.

Figure 18: Restarting the Switch


System > Reset
Reset
Click this button to reset the switch.
Save
Click this button to save current settings.
Factory Default Settings & Reboot
Click this button to return device to Factory Default Settings and reboot system.
Message from webpage
Note: It takes around 100~120 seconds to finish system reboot.
Do you want to reset the switch immediately?
OK
Cancel

5 INTERFACE CONFIGURATION

This chapter describes the following topics:

- Port Configuration – Configures connection settings, including auto-negotiation, or manual setting of speed, duplex mode, and flow control.
- Local Port Mirroring – Sets the source and target ports for mirroring on the local switch.
- Displaying Statistics – Shows Interface, Etherlike, and RMON port statistics in table or chart form.
- Cable Test – Tests the cable attached to a port.
- Trunk Configuration – Configures static or dynamic trunks.
- Saving Power – Adjusts the power provided to ports based on the length of the cable used to connect to other devices.

PORT CONFIGURATION

This section describes how to configure port connections, mirror traffic from one port to another, and run cable diagnostics.

CONFIGURING BY PORT LIST

Use the Interface > Port > General (Configure by Port List) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

COMMAND USAGE

- Auto-negotiation must be disabled before you can configure or force an interface to use the Speed/Duplex mode or Flow Control options.
- When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.
- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

- The Speed/Duplex mode is fixed at 1000full on the Gigabit SFP ports. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier.
- **Type** – Indicates the port type. (100Base-TX, 1000Base-T, 100Base SFP, 1000Base SFP)
- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Media Type** – Configures the forced/preferred port type to use for the combination ports (25-26 on the ES-2026/P and 21-24 on ES-2024G/P).
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port (even if a module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default for the combination ports.)
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
  - **10h** - Supports 10 Mbps half-duplex operation
  - **10f** - Supports 10 Mbps full-duplex operation
  - **100h** - Supports 100 Mbps half-duplex operation
  - **100f** - Supports 100 Mbps full-duplex operation
  - **1000f** (Gigabit ports only) - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames.
  - **FC** - Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex

operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.

Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

(Default: Autonegotiation enabled; Advertised capabilities for 100Base-TX – 10half, 10full, 100half, 100full; 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000Base-SX/LX/LH – 1000full)

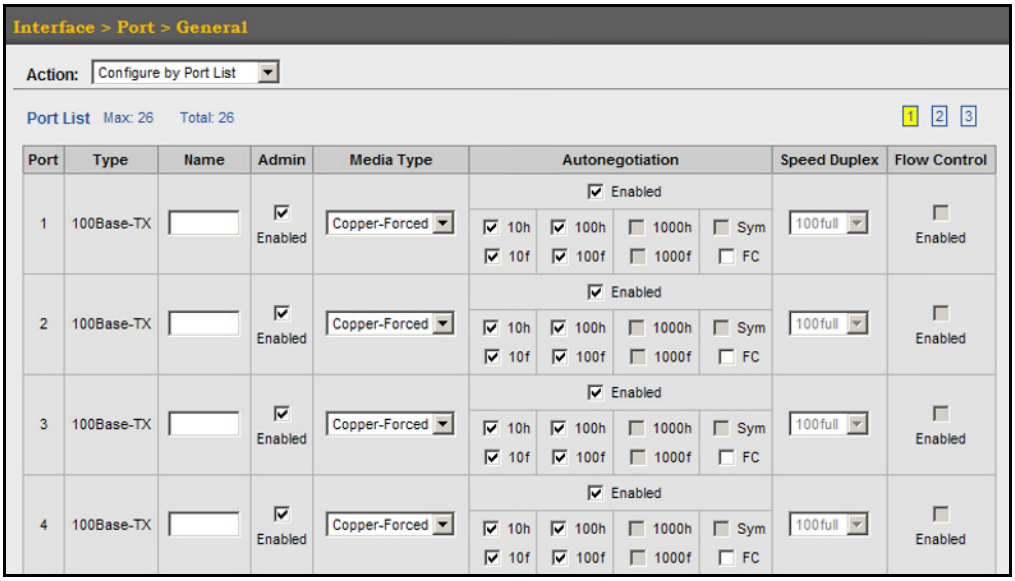
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
- **Flow Control** – Allows automatic or manual selection of flow control.

WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port List from the Action List.
3. Modify the required interface settings.
4. Click Apply.

Figure 19: Configuring Connections by Port List


Interface > Port > General
Action: Configure by Port List
Port List Max: 26 Total: 26
1 2 3
Port
Type
Name
Admin
Media Type
Autonegotiation
Speed Duplex
Flow Control
1 100Base-TX Enabled Copper-Forced Enabled 10h 100h 1000h Sym 10f 100f 1000f FC 100full Enabled
2 100Base-TX Enabled Copper-Forced Enabled 10h 100h 1000h Sym 10f 100f 1000f FC 100full Enabled
3 100Base-TX Enabled Copper-Forced Enabled 10h 100h 1000h Sym 10f 100f 1000f FC 100full Enabled
4 100Base-TX Enabled Copper-Forced Enabled 10h 100h 1000h Sym 10f 100f 1000f FC 100full Enabled

CONFIGURING BY PORT RANGE

Use the Interface > Port > General (Configure by Port Range) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

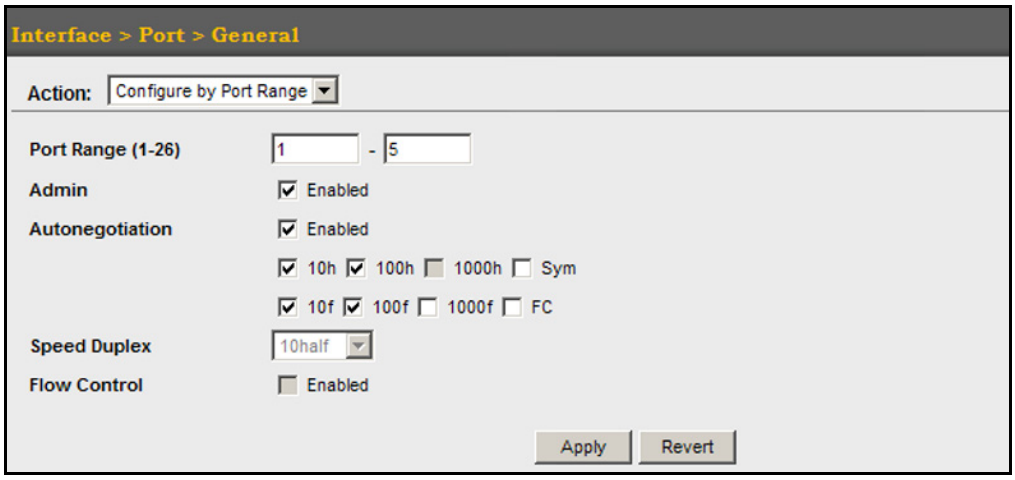
For more information on command usage and a description of the parameters, refer to "Configuring by Port List" on page 65.

WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port Range from the Action List.
3. Enter to range of ports to which your configuration changes apply.
4. Modify the required interface settings.
5. Click Apply.

Figure 20: Configuring Connections by Port Range



DISPLAYING CONNECTION STATUS

Use the Interface > Port > General (Show Information) page to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier.
- **Type** – Indicates the port type. (100Base-TX, 1000Base-T, 100Base SFP or 1000Base SFP)
- **Name** – Interface label.

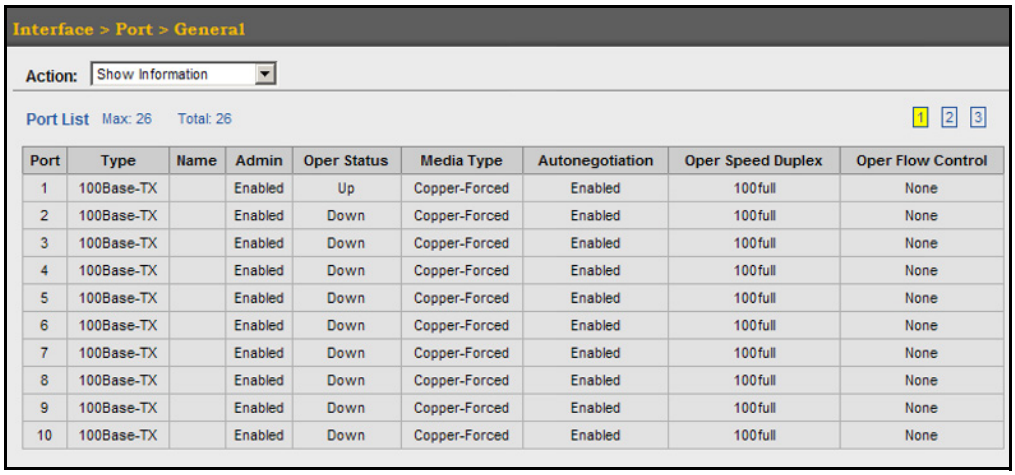
- **Admin** – Shows if the port is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Media Type** – Media type used.
  (Options: RJ-45 – Copper-Forced;
  Combination – Copper-Forced, SFP-Forced, or SFP-Preferred-Auto;
  Default: RJ-45 – Copper-Forced; Combination – SFP-Preferred-Auto)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Oper Speed Duplex** – Shows the current speed and duplex mode.
- **Oper Flow Control** – Shows if flow control is enabled or disabled.

WEB INTERFACE

To display port connection parameters:

1. Click Interface, Port, General.
2. Select Show Information from the Action List.

Figure 21: Displaying Port Information

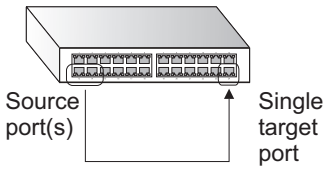


Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	100Base-TX		Enabled	Up	Copper-Forced	Enabled	100full	None
2	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
3	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
4	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
5	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
6	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
7	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
8	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
9	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
10	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None

CONFIGURING LOCAL PORT MIRRORING

Use the Interface > Port > Mirror page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Figure 22: Configuring Local Port Mirroring



COMMAND USAGE

- Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in this section).
- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.

PARAMETERS

These parameters are displayed:

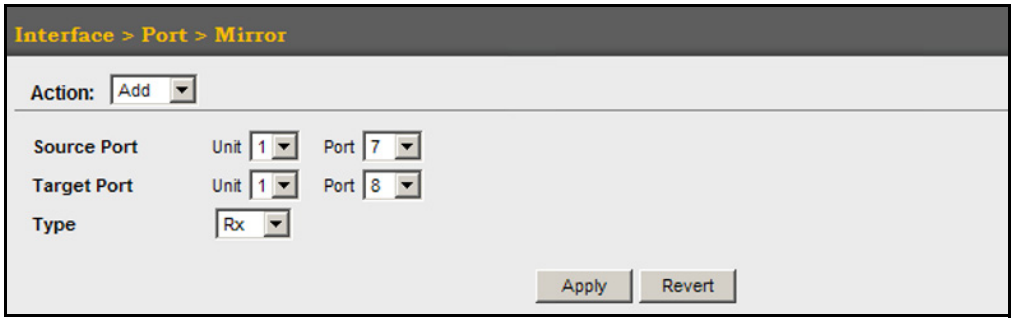
- **Source Port** – The port whose traffic will be monitored. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Target Port** – The port that will mirror the traffic on the source port. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)

WEB INTERFACE

To configure a local mirror session:

1. Click Interface, Port, Mirror.
2. Select Add from the Action List.
3. Specify the source port.
4. Specify the monitor port.
5. Specify the traffic type to be mirrored.
6. Click Apply.

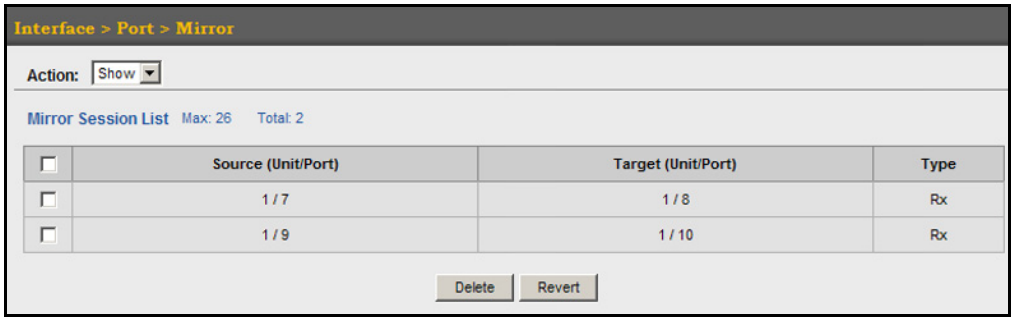
Figure 23: Configuring Local Port Mirroring



To display the configured mirror sessions:

1. Click Interface, Port, Mirror.
2. Select Show from the Action List.

Figure 24: Displaying Local Port Mirror Sessions



SHOWING PORT OR TRUNK STATISTICS

Use the Interface > Port/Trunk > Statistics or Chart page to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

NOTE: RMON groups 2, 3 and 9 can only be accessed using SNMP management software.

PARAMETERS

These parameters are displayed:

Table 5: Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.

Table 5: Port Statistics (Continued)

Parameter	Description
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Transmitted Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Etherlike Statistics	
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Alignment Errors	The number of alignment errors (missynchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.

Table 5: Port Statistics (Continued)

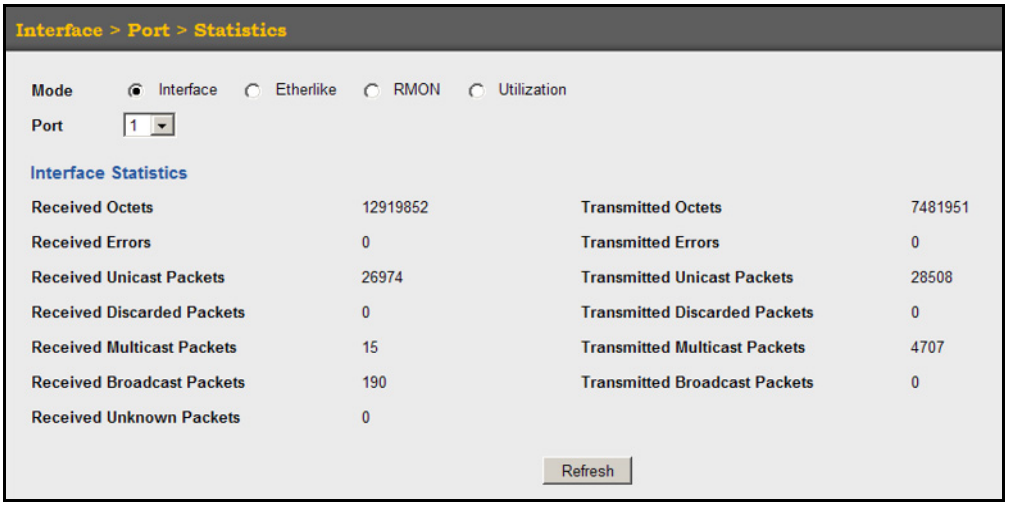
Parameter	Description
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
64 Bytes Packets	The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Packets 128-255 Byte Packets 256-511 Byte Packets 512-1023 Byte Packets 1024-1518 Byte Packets 1519-1536 Byte Packets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
Utilization Statistics	
Input Octets per second	Number of octets entering this interface per second.
Input Packets per second	Number of packets entering this interface per second.
Input Utilization	The input utilization rate for this interface.
Output Octets per second	Number of octets leaving this interface per second.
Output Packets per second	Number of packets leaving this interface per second.
Output Utilization	The output utilization rate for this interface.

WEB INTERFACE

To show a list of port statistics:

1. Click Interface, Port, Statistics.
2. Select the statistics mode to display (Interface, Etherlike, RMON or Utilization).
3. Select a port from the drop-down list.
4. Use the Refresh button at the bottom of the page if you need to update the screen.

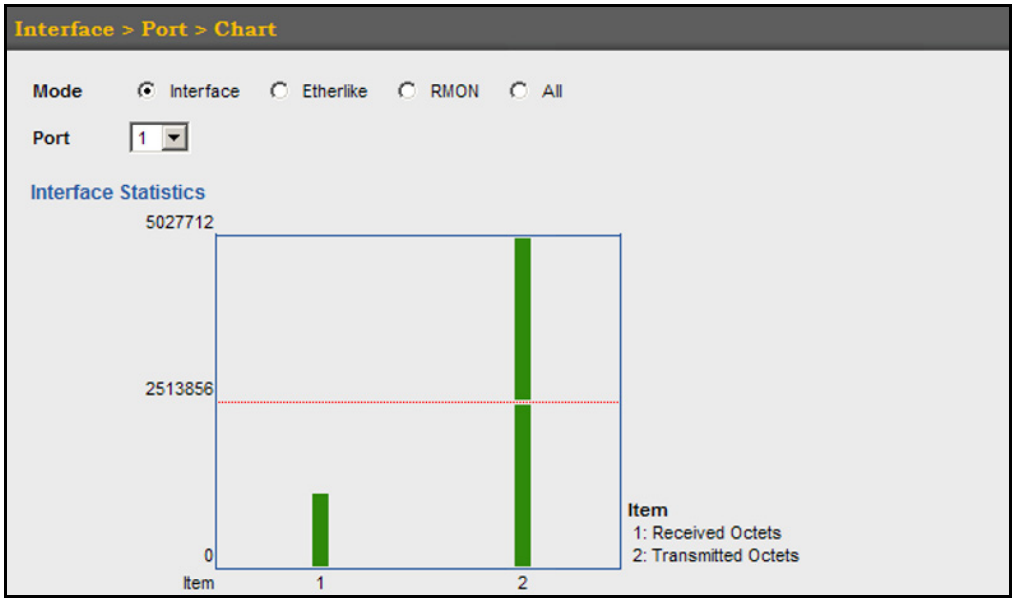
Figure 25: Showing Port Statistics (Table)



To show a chart of port statistics:

1. Click Interface, Port, Chart.
2. Select the statistics mode to display (Interface, Etherlike, RMON or All).
3. If Interface, Etherlike, RMON statistics mode is chosen, select a port from the drop-down list. If All (ports) statistics mode is chosen, select the statistics type to display.

Figure 26: Showing Port Statistics (Chart)



PERFORMING CABLE DIAGNOSTICS

Use the Interface > Port > Cable Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

COMMAND USAGE

- Cable diagnostics are performed using Time Domain Reflectometry (TDR) test methods. TDR analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- This cable test is only accurate for Fast Ethernet cables 50-140 meters long, and Gigabit Ethernet cables 0 - 250 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.

- Potential conditions which may be listed by the diagnostics include:
  - OK: Correctly terminated pair
  - Open: Open pair, no link partner
  - Short: Shorted pair
  - Not Supported: This message is displayed for any Fast Ethernet ports that are linked up, or for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
  - Impedance mismatch: Terminating impedance is not in the reference range.
- Ports are linked down while running cable diagnostics.

PARAMETERS

These parameters are displayed:

- **Port** – Switch port identifier. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Type** – Displays media type. (FE – Fast Ethernet, GE – Gigabit Ethernet)
- **Link Status** – Shows if the port link is up or down.
- **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- **Last Updated** – Shows the last time this port was tested.

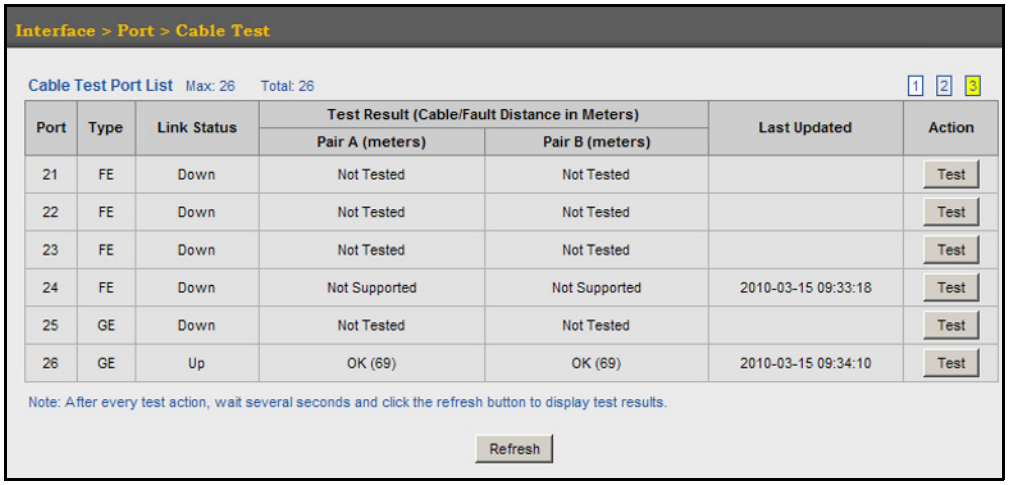
WEB INTERFACE

To test the cable attached to a port:

1. Click Interface, Port, Cable Test.

2. Click Test for any port to start the cable test.

Figure 27: Performing Cable Tests


Interface > Port > Cable Test
Cable Test Port List Max: 26 Total: 26
1 2 3
Port
Type
Link Status
Test Result (Cable/Fault Distance in Meters)
Pair A (meters)
Pair B (meters)
Last Updated
Action
21 FE Down Not Tested Not Tested Test
22 FE Down Not Tested Not Tested Test
23 FE Down Not Tested Not Tested Test
24 FE Down Not Supported Not Supported 2010-03-15 09:33:18 Test
25 GE Down Not Tested Not Tested Test
26 GE Up OK (69) OK (69) 2010-03-15 09:34:10 Test
Note: After every test action, wait several seconds and click the refresh button to display test results.
Refresh

TRUNK CONFIGURATION

This section describes how to configure static and dynamic trunks.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 12 trunks at a time on the switch.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

COMMAND USAGE

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use

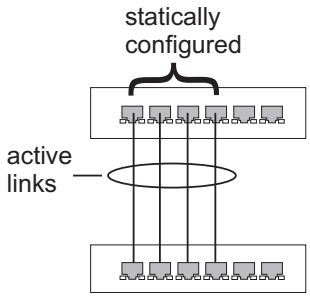
the web interface to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 12 trunks on a switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

CONFIGURING A STATIC TRUNK

Use the Interface > Trunk > Static page to create a trunk, assign member ports, and configure the connection parameters.

Figure 28: Configuring Static Trunks



COMMAND USAGE

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

PARAMETERS

These parameters are displayed:

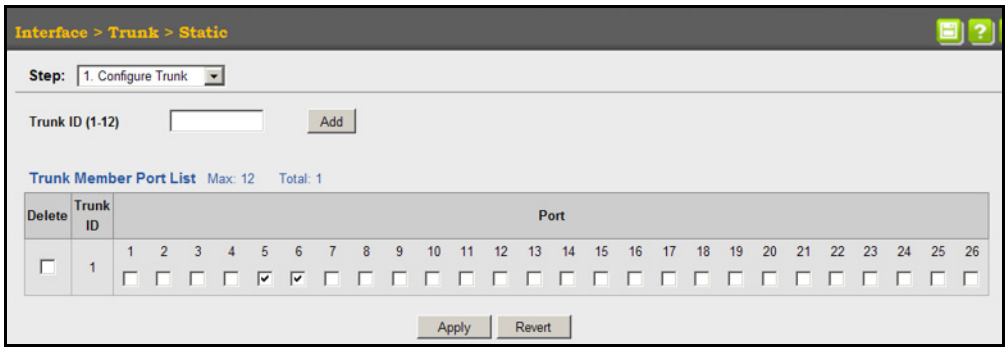
- **Trunk ID** – Trunk identifier. (Range: 1-12)
- **Trunk Member Port List** – The ports assigned to a trunk.

WEB INTERFACE

To create a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure Trunk from the Step list.
3. Enter a trunk identifier, and click Add.
4. Mark the ports assigned to each trunk.
5. Click Apply.

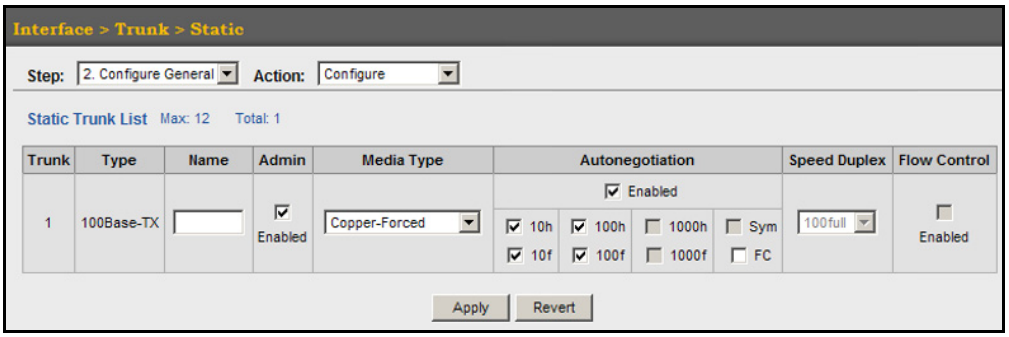
Figure 29: Creating Static Trunks


Interface > Trunk > Static
Step: 1. Configure Trunk
Trunk ID (1-12)
Add
Trunk Member Port List Max: 12 Total: 1
Delete
Trunk ID
Port
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
1
Apply
Revert

To configure connection parameters for a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Configure from the Action list.
4. Modify the required interface settings. (Refer to "Configuring by Port List" on page 65 for a description of the parameters.)
5. Click Apply.

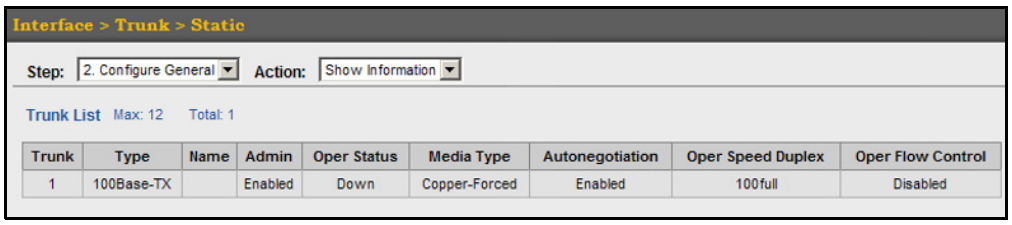
Figure 30: Configuring Connection Parameters for a Static Trunk



To show the static trunks configured on the switch:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Show Information from the Action list.

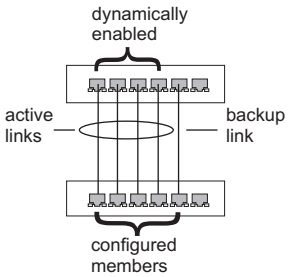
Figure 31: Showing Information for Static Trunks



CONFIGURING A DYNAMIC TRUNK

Use the Interface > Trunk > Dynamic (Configure Aggregator) page to set the administrative key for an aggregation group, enable LACP on a port, and configure protocol parameters for local and partner ports.

Figure 32: Configuring Dynamic Trunks



COMMAND USAGE

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.

NOTE: If the LACP admin key is not set when a channel group is formed (i.e., it has a null value of 0), the operational value of this key is set to the same value as the port admin key used by the interfaces that joined the group.

PARAMETERS

These parameters are displayed:

Configure Aggregator

- **Admin Key** – LACP administration key is used to identify a specific link aggregation group (LAG) during local LACP setup on the switch. (Range: 0-65535)

Configure Aggregation Port - General

- **Port** – Port identifier. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **LACP Status** – Enables or disables LACP on a port.

Configure Aggregation Port - Actor/Partner

- **Port** – Port number. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)

  By default, the Actor Admin Key is determined by port's link speed, and copied to Oper Key. The Partner Admin Key is assigned to zero, and the Oper Key is set based upon LACP PDUs received from the Partner.
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to

other switches during LAG negotiations. (Range: 0-65535; Default: 32768)

System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.

- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

NOTE: Configuring LACP settings for a port only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with that port.

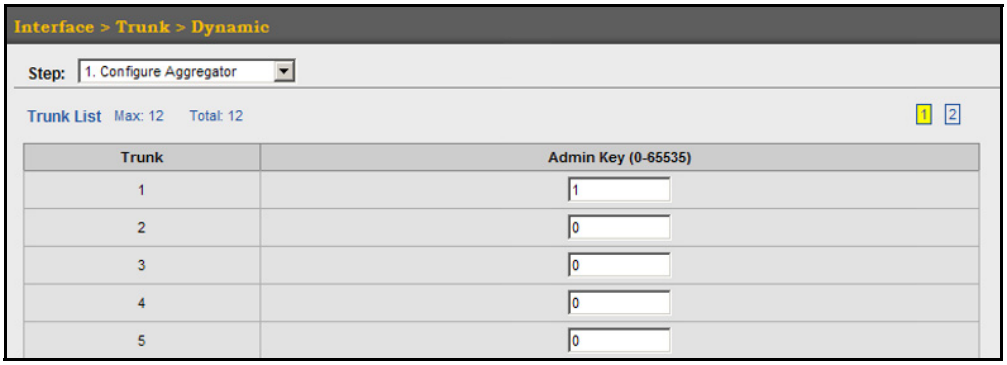
NOTE: Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

WEB INTERFACE

To configure the admin key for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregator from the Step list.
3. Set the Admin Key for the required LACP group.
4. Click Apply.

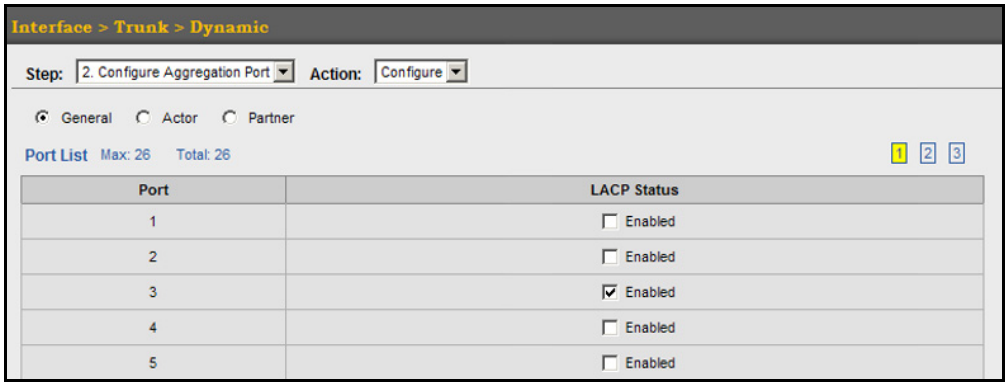
Figure 33: Configuring the LACP Aggregator Admin Key



To enable LACP for a port:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click General.
5. Enable LACP on the required ports.
6. Click Apply.

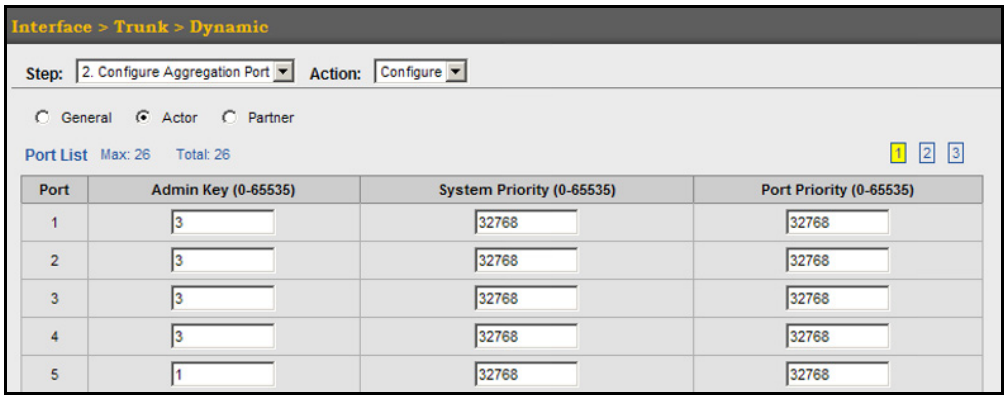
Figure 34: Enabling LACP on a Port



To configure LACP parameters for group members:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click Actor or Partner.
5. Configure the required settings.
6. Click Apply.

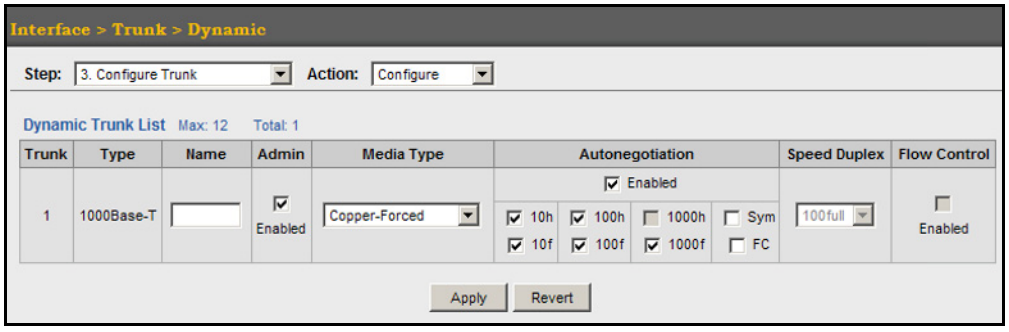
Figure 35: Configuring LACP Parameters on a Port



To configure the connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step list.
3. Select Configure from the Action list.
4. Modify the required interface settings. (Refer to "Configuring by Port List" on page 65 for a description of the parameters.)
5. Click Apply.

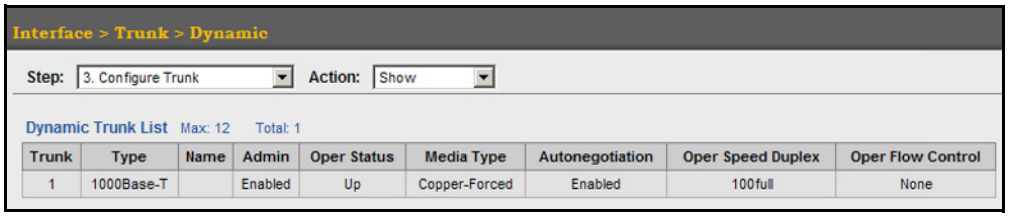
Figure 36: Configuring Connection Parameters for a Dynamic Trunk



To show the connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step list.
3. Select Show from the Action list.

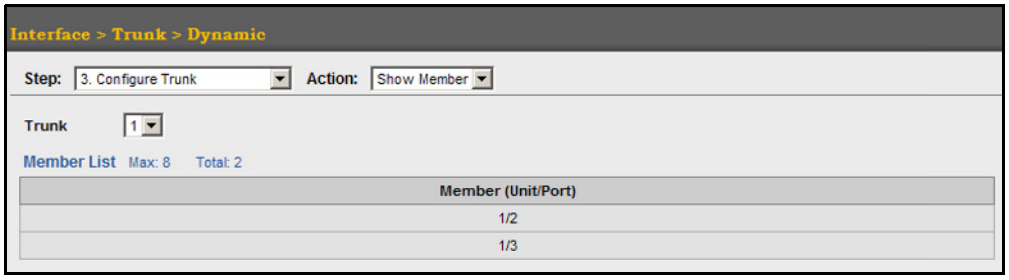
Figure 37: Showing Connection Parameters for Dynamic Trunks



To show the port members of dynamic trunks:

1. Click Interface, Trunk, Dynamic.
2. Select Configure General from the Step list.
3. Select Show Member from the Action list.

Figure 38: Showing Members of Dynamic Trunks



DISPLAYING LACP PORT COUNTERS

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Counters) page to display statistics for LACP protocol messages.

PARAMETERS

These parameters are displayed:

Table 6: LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.

Table 6: LACP Port Counters (Continued)

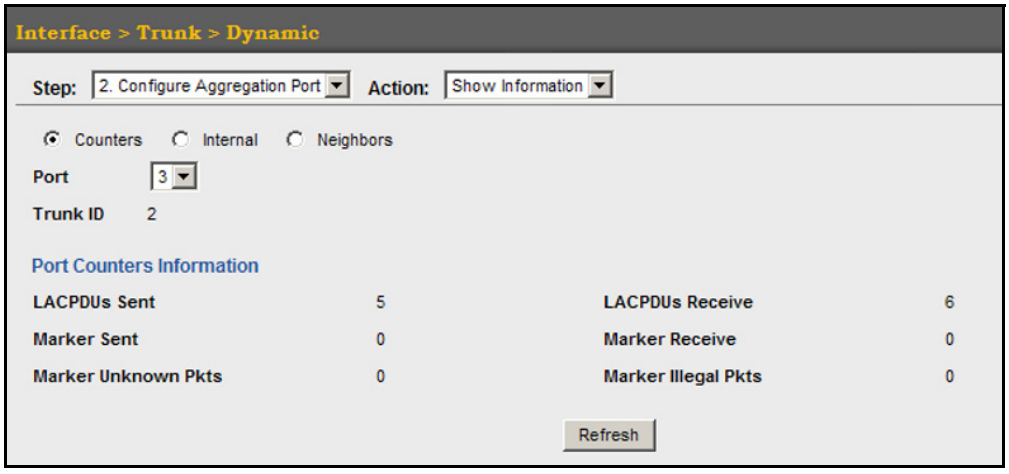
Parameter	Description
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

WEB INTERFACE

To display LACP port counters:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Counters.
5. Select a group member from the Port list.

Figure 39: Displaying LACP Port Counters



DISPLAYING LACP SETTINGS AND STATUS FOR THE LOCAL SIDE

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Internal) page to display the configuration settings and operational state for the local side of a link aggregation.

PARAMETERS

These parameters are displayed:

Table 7: LACP Internal Configuration Information

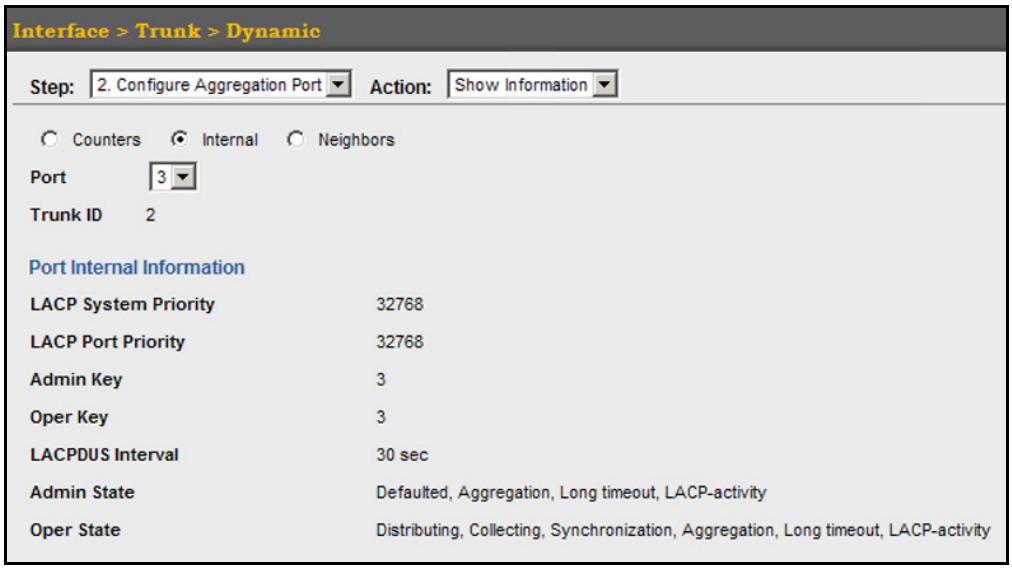
Parameter	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.
LACPDUs Interval	Number of seconds before invalidating received LACPDU information.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ Expired – The actor's receive machine is in the expired state; ◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. ◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. ◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. ◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. ◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. ◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. ◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

WEB INTERFACE

To display LACP settings and status for the local side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Internal.
5. Select a group member from the Port list.

Figure 40: Displaying LACP Port Internal Information



DISPLAYING LACP SETTINGS AND STATUS FOR THE REMOTE SIDE

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Neighbors) page to display the configuration settings and operational state for the remote side of a link aggregation.

PARAMETERS

These parameters are displayed:

Table 8: LACP Internal Configuration Information

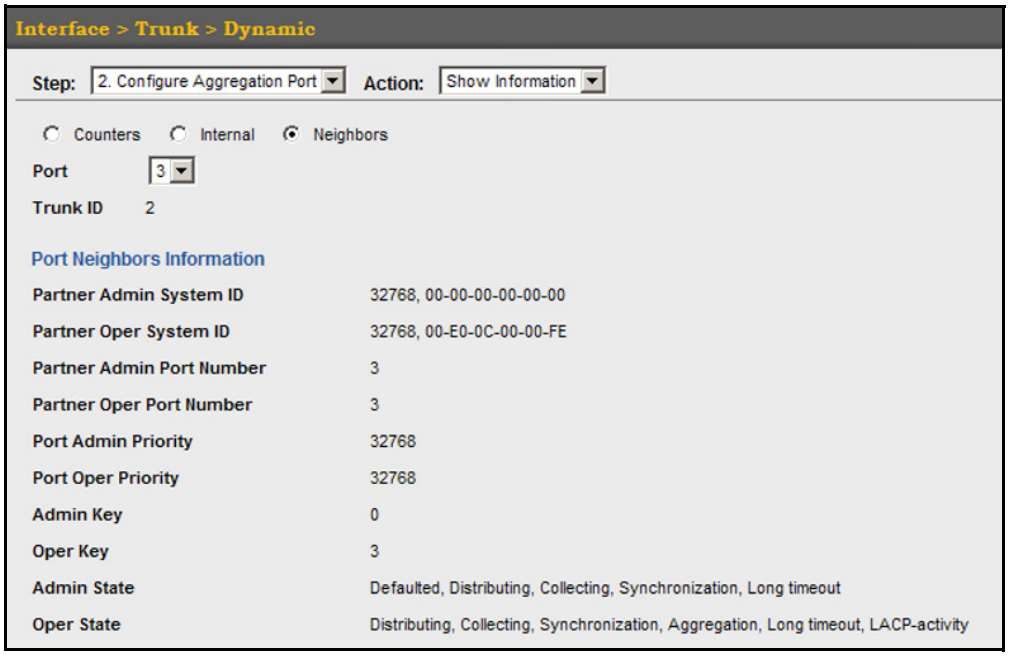
Parameter	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

WEB INTERFACE

To display LACP settings and status for the remote side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Internal.
5. Select a group member from the Port list.

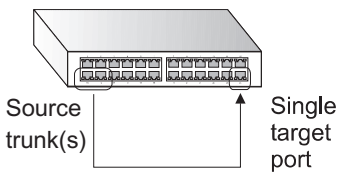
Figure 41: Displaying LACP Port Remote Information


Interface > Trunk > Dynamic
Step: 2. Configure Aggregation Port
Action: Show Information
Counters
Internal
Neighbors
Port 3
Trunk ID 2
Port Neighbors Information
Partner Admin System ID 32768, 00-00-00-00-00-00
Partner Oper System ID 32768, 00-E0-0C-00-00-FE
Partner Admin Port Number 3
Partner Oper Port Number 3
Port Admin Priority 32768
Port Oper Priority 32768
Admin Key 0
Oper Key 3
Admin State Defaulted, Distributing, Collecting, Synchronization, Long timeout
Oper State Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

CONFIGURING TRUNK MIRRORING

Use the Interface > Trunk > Mirror page to mirror traffic from any source trunk to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source trunk in a completely unobtrusive manner.

Figure 42: Configuring Trunk Mirroring



COMMAND USAGE

- Traffic can be mirrored from one or more source trunks to a destination port on the same switch.
- Monitor port speed should match or exceed source trunk speed, otherwise traffic may be dropped from the monitor port.

PARAMETERS

These parameters are displayed:

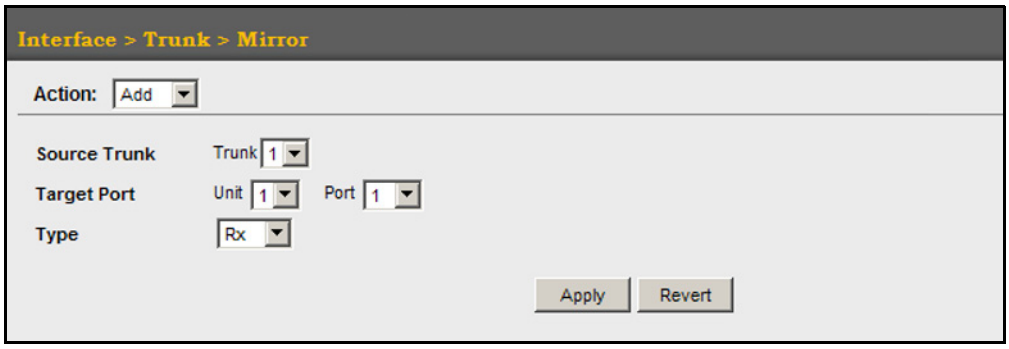
- **Source Trunk** – The trunk whose traffic will be monitored. (Range: 1-12)
- **Target Port** – The port that will mirror the traffic on the source trunk. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)

WEB INTERFACE

To configure a local mirror session:

1. Click Interface, Trunk, Mirror.
2. Select Add from the Action List.
3. Specify the source trunk.
4. Specify the monitor port.
5. Specify the traffic type to be mirrored.
6. Click Apply.

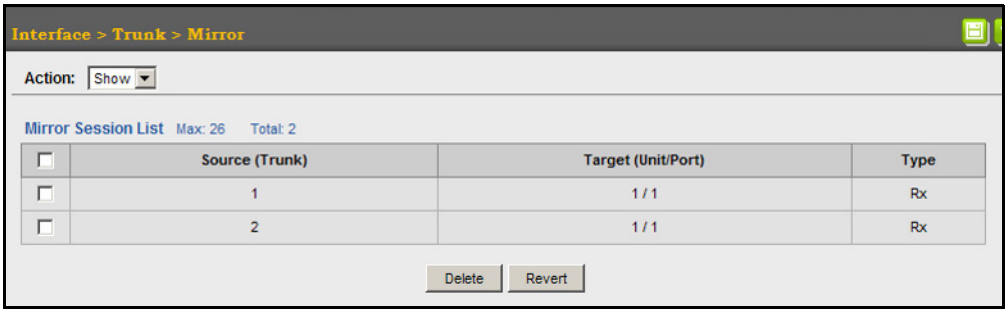
Figure 43: Configuring Trunk Mirroring



To display the configured mirror sessions:

1. Click Interface, Trunk, Mirror.
2. Select Show from the Action List.

Figure 44: Displaying Trunk Mirror Sessions



SAVING POWER

Use the Interface > Green Ethernet page to enable power savings mode on the selected port.

COMMAND USAGE

- IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.
- The power-saving methods provided by this switch include:
  - Power saving when there is no link partner:

    Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

  - Power saving when there is a link partner:

    Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch

analyzes cable length to determine whether or not it can reduce the signal amplitude used on a particular link.

NOTE: Power savings can only be implemented on Gigabit Ethernet ports when using twisted-pair cabling. Power-savings mode on a active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

PARAMETERS

These parameters are displayed:

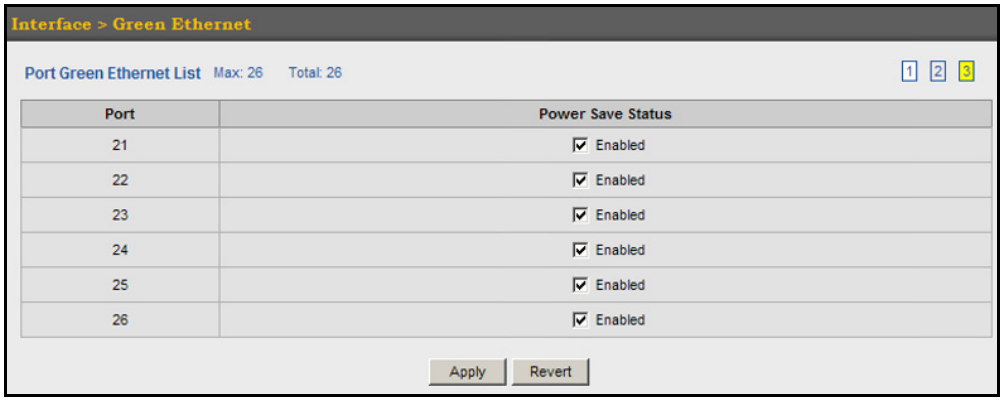
- **Port** – Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- **Power Saving Status** – Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements. (Default: Enabled on Gigabit Ethernet RJ-45 ports)

WEB INTERFACE

To enable power savings:

1. Click Interface, Green Ethernet.
2. Mark the Enabled check box for a port.
3. Click Apply.

Figure 45: Enabling Power Savings



6 VLAN CONFIGURATION

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 128 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

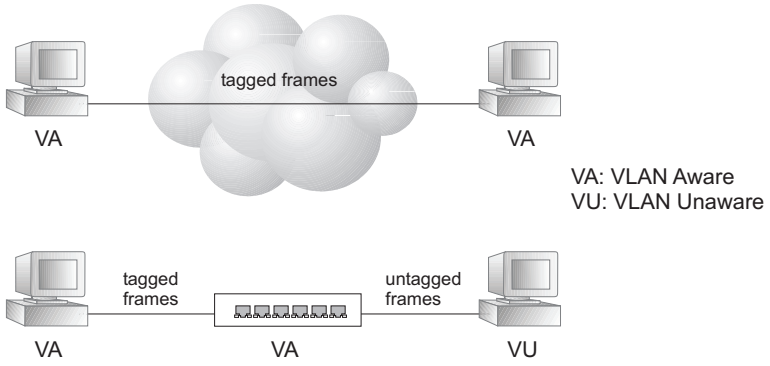
Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate

network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

NOTE: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

Figure 46: VLAN Compliant and VLAN Non-compliant Devices



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

CONFIGURING VLAN GROUPS

Use the VLAN > Static (Configure VLAN) page to create or remove VLAN groups, or set administrative status. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

PARAMETERS

These parameters are displayed:

- **VLAN ID** – ID of VLAN or range of VLANs (1-4093).

  Up to 128 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

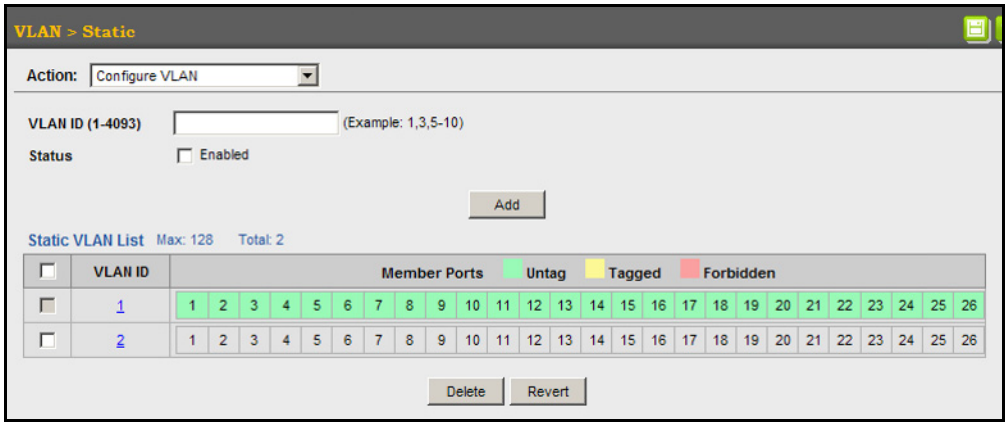
- **Status** – Enables or disables the specified VLAN.

WEB INTERFACE

To create VLAN groups:

1. Click VLAN, Static.
2. Select Configure VLAN from the Action list.
3. Enter a VLAN ID or range of IDs.
4. Mark Enabled to configure the VLAN as operational.
5. Click Add.

Figure 47: Creating Static VLANs



ADDING STATIC MEMBERS TO VLANS

Use the VLAN > Static (Modify VLAN and Member Ports, Edit Member by Interface, or Edit Member by Interface Range) pages to configure port members for the selected VLAN index, interface, or a range of interfaces. Use the menus for editing port members to configure the VLAN behavior for specific interfaces, including the mode of operation (Hybrid or 1Q Trunk), the default VLAN identifier (PVID), accepted frame types, and ingress filtering. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices.

PARAMETERS

These parameters are displayed:

Modify VLAN and Member Ports

- **VLAN** – ID of configured VLAN (1-4093).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-12)
- **Mode** – Indicates VLAN membership mode for an interface. (Default: Access)
  - **Access** - Sets the port to operate as an untagged interface. The port transmits and receives untagged frames on a single VLAN only.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits

tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)

- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:

  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.



NOTE: VLAN 1 is the default untagged VLAN containing all ports on the switch using Access mode.

Edit Member by Interface

All parameters are the same as those described under the preceding section for Modify VLAN and Member Ports.

Edit Member by Interface Range

All parameters are the same as those described under the earlier section for Modify VLAN and Member Ports, except for the items shown below.

- **Port Range** – Displays a list of ports. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **Trunk Range** – Displays a list of ports. (Range: 1-12)

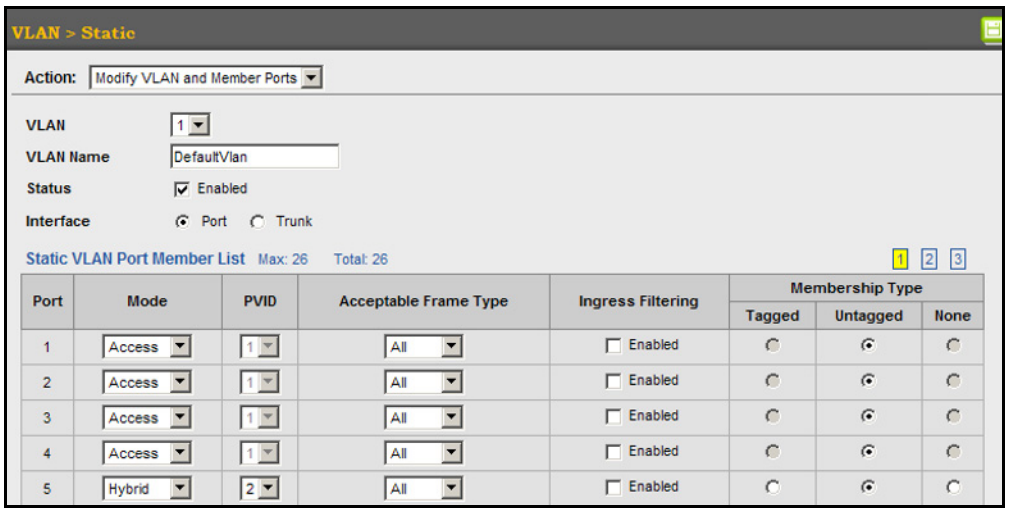
NOTE: The PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.

WEB INTERFACE

To configure static members by the VLAN index:

1. Click VLAN, Static.
2. Select Modify VLAN and Member Ports from the Action list.
3. Set the Interface type to display as Port or Trunk.
4. Modify the settings for any interface as required. Remember that Membership Type cannot be changed until an interface has been added to another VLAN and the PVID changed to anything other than 1.
5. Click Apply.

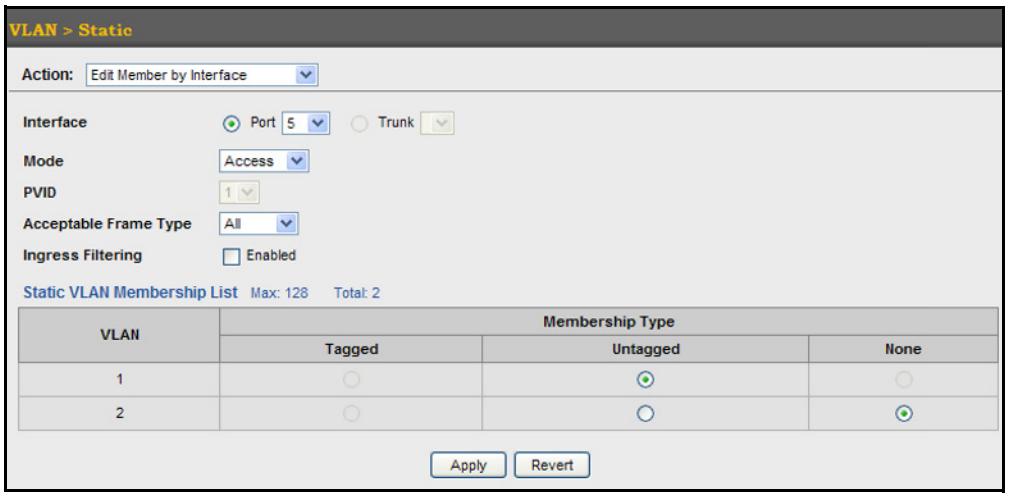
Figure 48: Configuring Static Members by VLAN Index



To configure static members by interface:

1. Click VLAN, Static.
2. Select Edit Member by Interface from the Action list.
3. Select a port or trunk configure.
4. Modify the settings for any interface as required.
5. Click Apply.

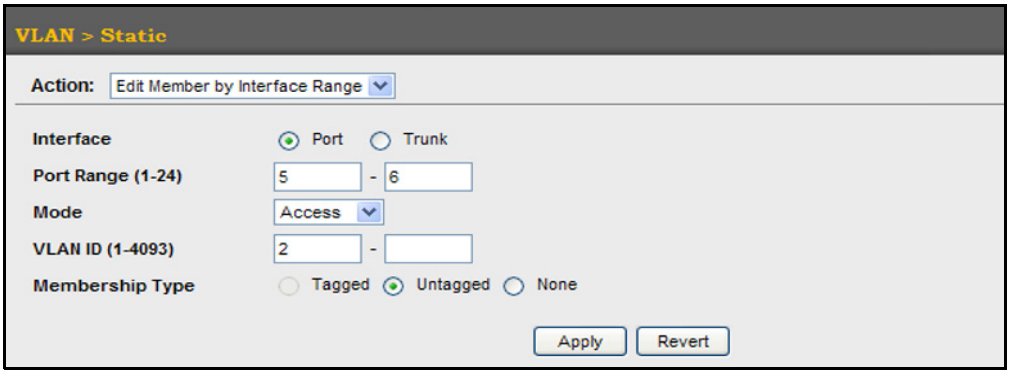
Figure 49: Configuring Static VLAN Members by Interface



To configure static members by interface range:

1. Click VLAN, Static.
2. Select Edit Member by Interface Range from the Action list.
3. Set the Interface type to display as Port or Trunk.
4. Enter an interface range.
5. Modify the VLAN parameters as required. Remember that the PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.
6. Click Apply.

Figure 50: Configuring Static VLAN Members by Interface Range



7 ADDRESS TABLE SETTINGS

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

This chapter describes the following topics:

- Static MAC Addresses – Configures static entries in the address table.
- Address Aging Time – Sets time out for dynamically learned entries.
- Dynamic Address Cache – Shows dynamic entries in the address table.

SETTING STATIC ADDRESSES

Use the MAC Address > Static page to configure static MAC addresses. A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- Static addresses will not be removed from the address table when a given interface link is down.
- A static address cannot be learned on another port until the address is removed from the table.

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of configured VLAN. (Range: 1-4093)

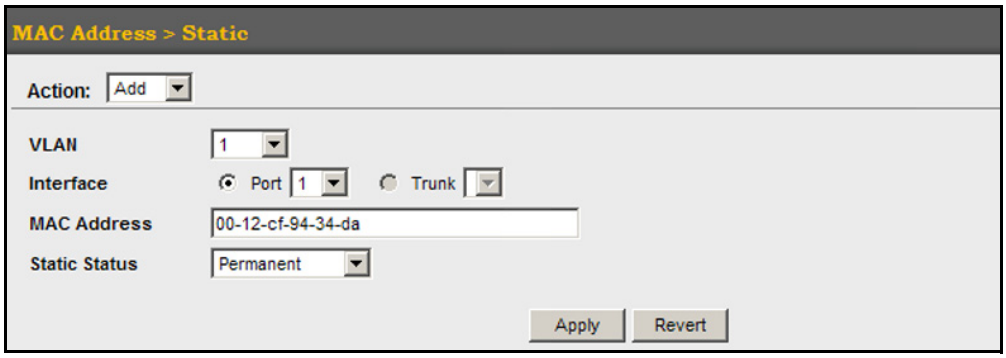
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **Static Status** – Sets the time to retain the specified address.
  - Delete-on-reset - Assignment lasts until the switch is reset.
  - Permanent - Assignment is permanent. (This is the default.)

WEB INTERFACE

To configure a static MAC address:

1. Click MAC Address, Static.
2. Select Add from the Action list.
3. Specify the VLAN, the port or trunk to which the address will be assigned, the MAC address, and the time to retain this entry.
4. Click Apply.

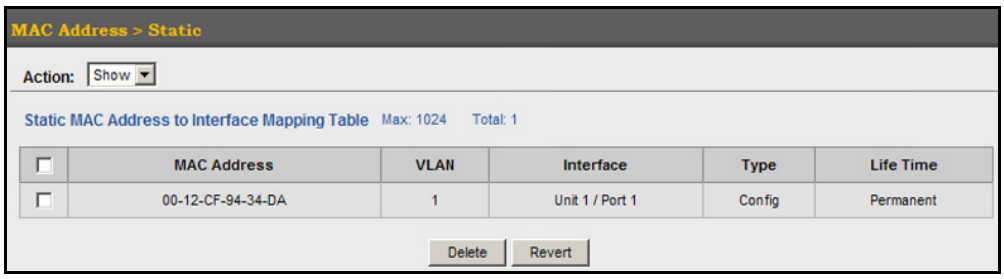
Figure 51: Configuring Static MAC Addresses



To show the static addresses in MAC address table:

1. Click MAC Address, Static.
2. Select Show from the Action list.

Figure 52: Displaying Static MAC Addresses



CHANGING THE AGING TIME

Use the MAC Address > Dynamic (Configure Aging) page to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

PARAMETERS

These parameters are displayed:

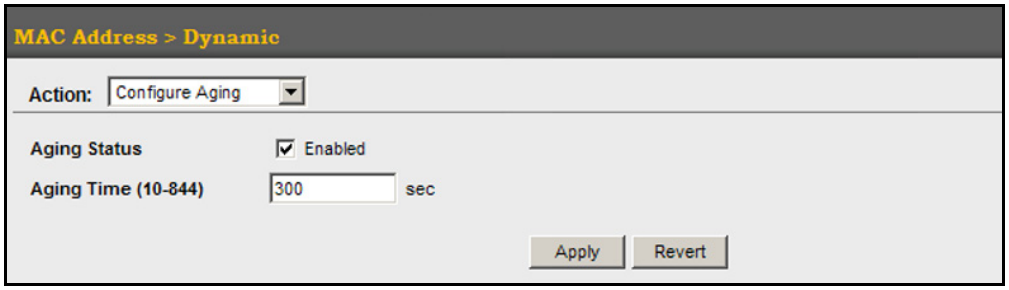
- **Aging Status** – Enables/disables the function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-844 seconds; Default: 300 seconds)

WEB INTERFACE

To set the aging time for entries in the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Configure Aging from the Action list.
3. Modify the aging status if required.
4. Specify a new aging time.
5. Click Apply.

Figure 53: Setting the Address Aging Time



DISPLAYING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Show Dynamic MAC) page to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

PARAMETERS

These parameters are displayed:

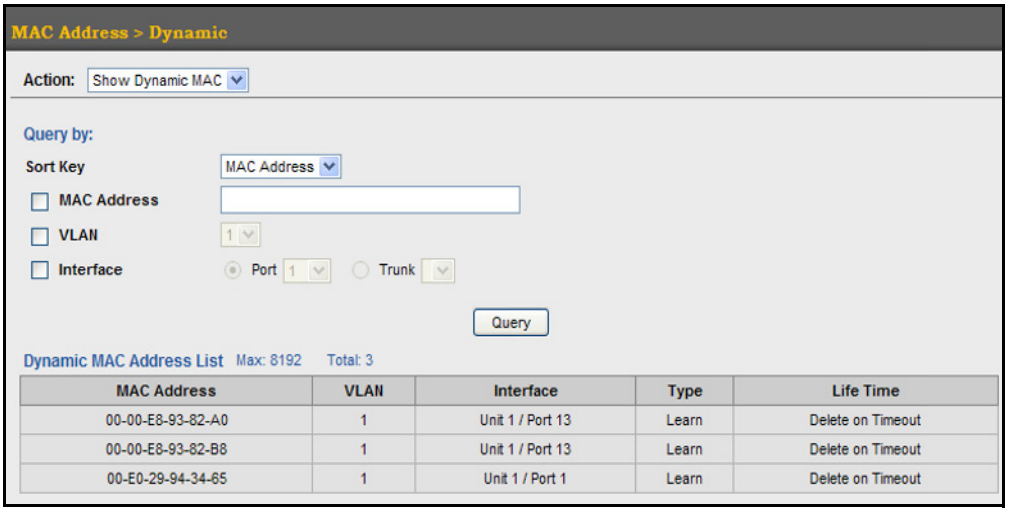
- **Sort Key** - You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Interface** – Indicates a port or trunk.
- **Type** – Shows that the entries in this table are learned.
- **Life Time** – Shows the time to retain the specified address.

WEB INTERFACE

To show the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Show Dynamic MAC from the Action list.
3. Select the Sort Key (MAC Address, VLAN, or Interface).
4. Enter the search parameters (MAC Address, VLAN, or Interface).
5. Click Query.

Figure 54: Displaying the Dynamic MAC Address Table


MAC Address > Dynamic
Action: Show Dynamic MAC
Query by:
Sort Key MAC Address
MAC Address
VLAN 1
Interface Port 1 Trunk
Query
Dynamic MAC Address List Max: 8192 Total: 3
MAC Address | VLAN | Interface | Type | Life Time
00-00-E8-93-82-A0 | 1 | Unit 1 / Port 13 | Learn | Delete on Timeout
00-00-E8-93-82-B8 | 1 | Unit 1 / Port 13 | Learn | Delete on Timeout
00-E0-29-94-34-65 | 1 | Unit 1 / Port 1 | Learn | Delete on Timeout

CLEARING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Clear Dynamic MAC) page to remove any learned entries from the forwarding database.

PARAMETERS

These parameters are displayed:

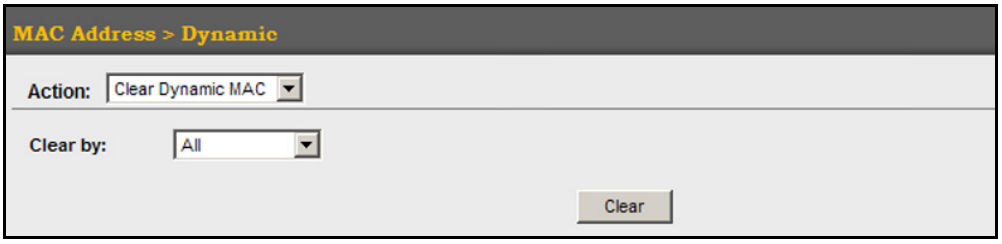
- **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or trunk.

WEB INTERFACE

To clear the entries in the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Clear Dynamic MAC from the Action list.
3. Select the method by which to clear the entries (i.e., All, MAC Address, VLAN, or Interface).
4. Enter information in the additional fields required for clearing entries by MAC Address, VLAN, or Interface.
5. Click Clear.

Figure 55: Clearing Entries in the Dynamic MAC Address Table



8 SPANNING TREE ALGORITHM

This chapter describes the following basic topics:

- Global Settings for STA – Configures global bridge settings for STP, RSTP and MSTP.
- Interface Settings for STA – Configures interface settings for STA, including priority, path cost, link type, and designation as an edge port.

OVERVIEW

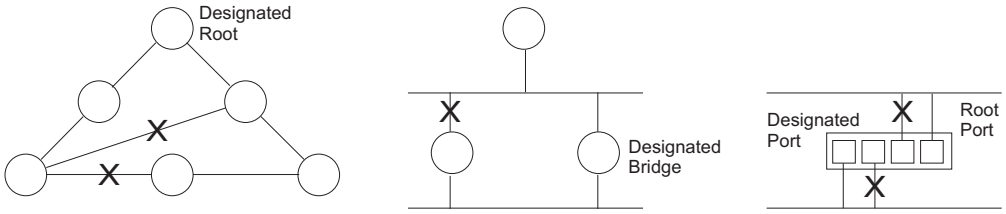
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Figure 56: STP Root Ports and Designated Ports



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

CONFIGURING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Configure) page to configure global settings for the spanning tree that apply to the entire switch.

COMMAND USAGE

- Spanning Tree Protocol[1]

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

- Rapid Spanning Tree Protocol[1]

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

1. STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

PARAMETERS

These parameters are displayed:

Basic Configuration of Global Settings

- **Spanning Tree Status** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Advanced Configuration Settings

The following attributes are based on RSTP, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP:

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

When the Switch Becomes Root

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)]
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

WEB INTERFACE

To configure global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes. Note that the parameters displayed for the spanning tree types (STP and RSTP) varies as described in the preceding section.
5. Click Apply

Figure 57: Configuring Global Settings for STA (STP)

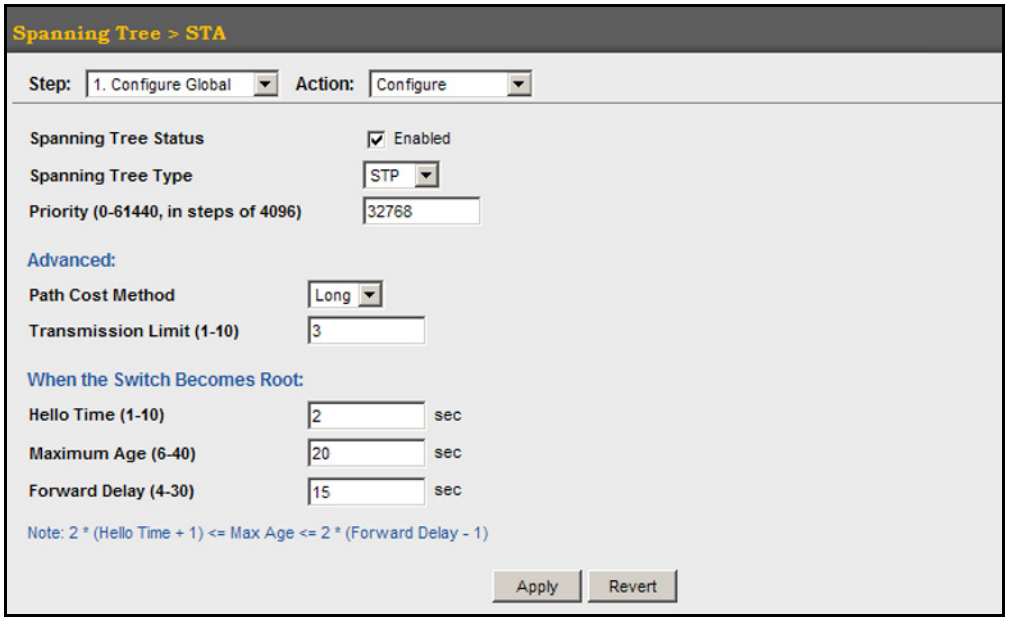
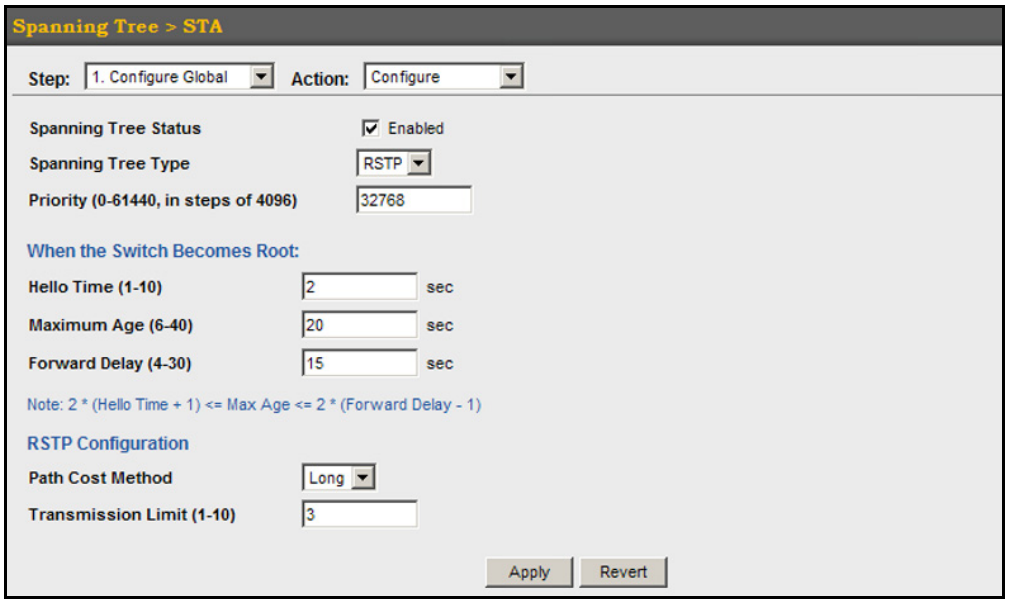


Figure 58: Configuring Global Settings for STA (RSTP)



DISPLAYING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Show Information) page to display a summary of the current bridge STA information that applies to the entire switch.

PARAMETERS

The parameters displayed are described in the preceding section, except for the following items:

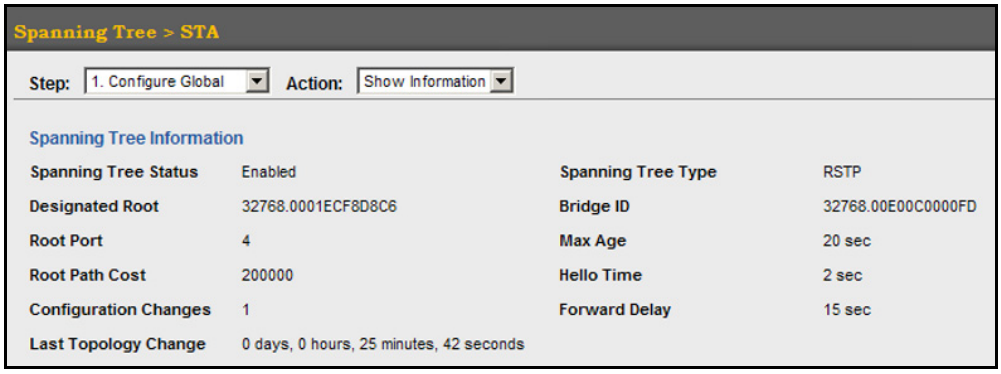
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, and MAC address (where the address is taken from the switch system).
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

WEB INTERFACE

To display global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.

Figure 59: Displaying Global Settings for STA


Spanning Tree > STA
Step: 1. Configure Global
Action: Show Information
Spanning Tree Information
Spanning Tree Status Enabled
Spanning Tree Type RSTP
Designated Root 32768.0001ECF8D8C6
Bridge ID 32768.00E00C0000FD
Root Port 4
Max Age 20 sec
Root Path Cost 200000
Hello Time 2 sec
Configuration Changes 1
Forward Delay 15 sec
Last Topology Change 0 days, 0 hours, 25 minutes, 42 seconds

CONFIGURING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Configure) page to configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.
- **Admin Edge Status for all ports** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Enabled)
  - **Enabled** – Manually configures a port as an Edge Port.

- **Disabled** – Disables the Edge Port setting.
- **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP BPDU. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages (see maximum age under "Configuring Global Settings for STA" on page 108).

An interface cannot function as an edge port under the following conditions:

- If spanning tree mode is set to STP (page 108), edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
- If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
- If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state (see "Displaying Interface Settings for STA" on page 116).

◆ **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)

◆ **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

- Default: 128
- Range: 0-240, in steps of 16

◆ **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method[2], 1-200,000,000 for the long path cost method)

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default

2. Refer to "Configuring Global Settings for STA" on page 108 for information on setting the path cost method.

path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 9: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 10: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000

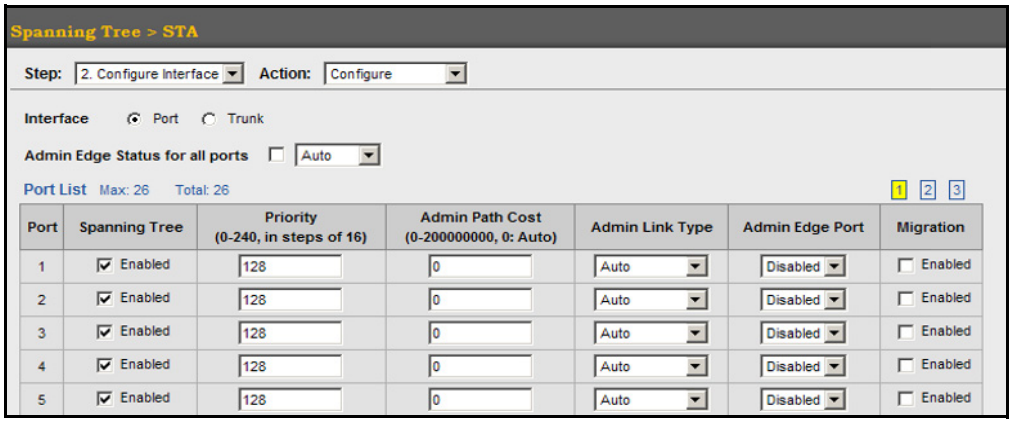
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port** – Refer to "Admin Edge Status for all ports" at the beginning of this section.
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

WEB INTERFACE

To configure interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes.
5. Click Apply.

Figure 60: Configuring Interface Settings for STA


Spanning Tree > STA
Step: 2. Configure Interface Action: Configure
Interface Port Trunk
Admin Edge Status for all ports Auto
Port List Max: 26 Total: 26
1 2 3
Port
Spanning Tree
Priority (0-240, in steps of 16)
Admin Path Cost (0-200000000, 0: Auto)
Admin Link Type
Admin Edge Port
Migration
1 Enabled 128 0 Auto Disabled Enabled
2 Enabled 128 0 Auto Disabled Enabled
3 Enabled 128 0 Auto Disabled Enabled
4 Enabled 128 0 Auto Disabled Enabled
5 Enabled 128 0 Auto Disabled Enabled

DISPLAYING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Show Information) page to display the current status of ports or trunks in the Spanning Tree.

PARAMETERS

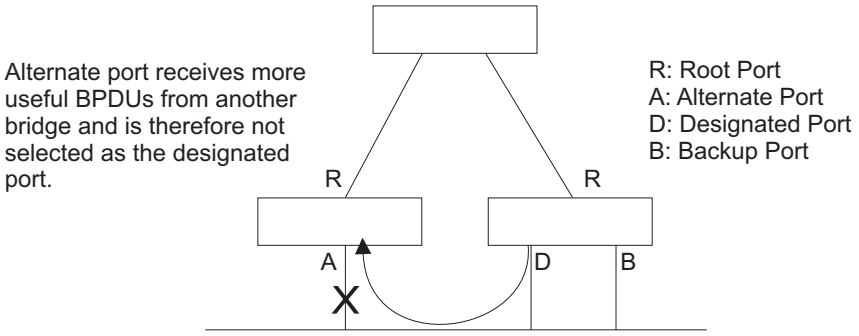
These parameters are displayed:

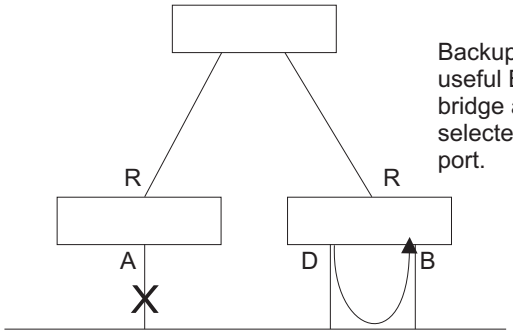
- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

  The rules defining port status are:
  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 113.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 113 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

Figure 61: STA Port Roles



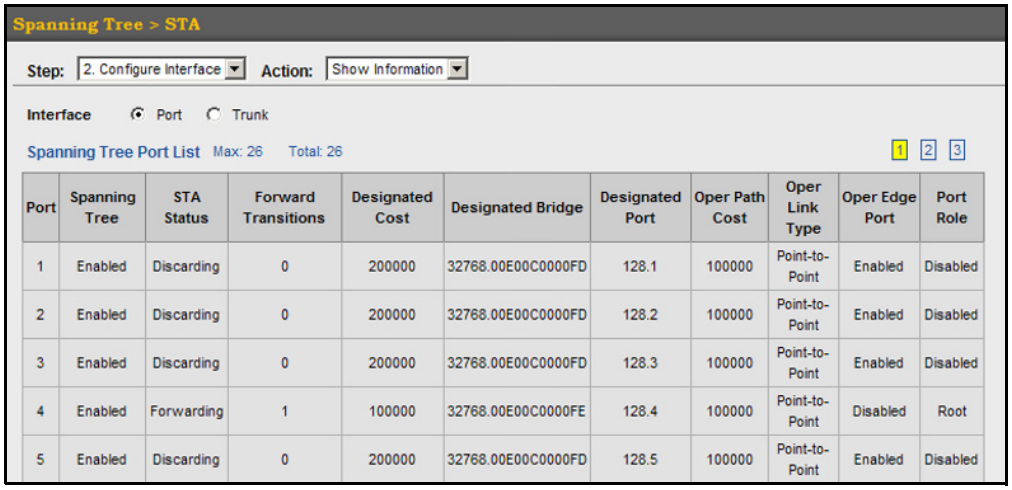


WEB INTERFACE

To display interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 62: Displaying Interface Settings for STA


Spanning Tree > STA
Step: 2. Configure Interface
Action: Show Information
Interface Port Trunk
Spanning Tree Port List Max: 26 Total: 26
1 2 3

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.1	100000	Point-to-Point	Enabled	Disabled
2	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.2	100000	Point-to-Point	Enabled	Disabled
3	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.3	100000	Point-to-Point	Enabled	Disabled
4	Enabled	Forwarding	1	100000	32768.00E00C0000FE	128.4	100000	Point-to-Point	Disabled	Root
5	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.5	100000	Point-to-Point	Enabled	Disabled

9 RATE LIMIT CONFIGURATION

Use the Traffic > Rate Limit page to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

COMMAND USAGE

The ASIC used to control the ingress rate limit has a default time frame of 1 ms, 10 ms, 100 ms, and 1 second respectively for 10 Gbps, 1 Gbps, 100 Mbps, and 10 Mbps connection rates. Ingress rate limiting is processed 100 times per second (also referred to as 100 scales per second), regardless of the packet size.

NOTE: Egress rate limiting does not function in this manner.

For example, a Gigabit port has a 10 ms window size, so there are 100 scales per second, each scale having a bandwidth of 10 Mbps, and using an inter-packet gap of 20 bytes.

Therefore, when the rate limit is set at 64 kbit/s, each scale has a shared bandwidth of 80 bytes.

When the packet size = 64 bytes, and the gap = 20 bytes,
each packet = 84 bytes > 80bytes. Only one packet can pass through in each scale. One second has 100 scales, so the rate is 100 packets per second.

When the packet size = 640 bytes, and the gap = 20 bytes,
each packet = 660 bytes > 80 bytes. The switch will only let one packet pass in each scale, so there are still 100 packets per second.

When the packet size = 1500 bytes, and the gap = 20 bytes,
each packet = 1520 bytes > 80 bytes. The switch will only let one packet pass in each scale, so there are still 100 packets per second.

The following table shows the actual number of packets received when various ingress rate limits are applied to packets of different sizes. The values shown below were measured for both ingress rate limiting and storm control functions.

Table 11: Effective Rate Limit

Packet Size	Rate Limit	Packets Received
64 bytes	64 kbit/s	100
	128 kbit/s	200
	256 kbit/s	400
	512 kbit/s	800
	1024 kbit/s	1600
	2048 kbit/s	3105
128 bytes	64 kbit/s	100
	128 kbit/s	100
	256 kbit/s	300
	512 kbit/s	500
	1024 kbit/s	900
	2048 kbit/s	1800
512 bytes	64 kbit/s	100
	128 kbit/s	100
	256 kbit/s	100
	512 kbit/s	200
	1024 kbit/s	300
	2048 kbit/s	500

PARAMETERS

These parameters are displayed:

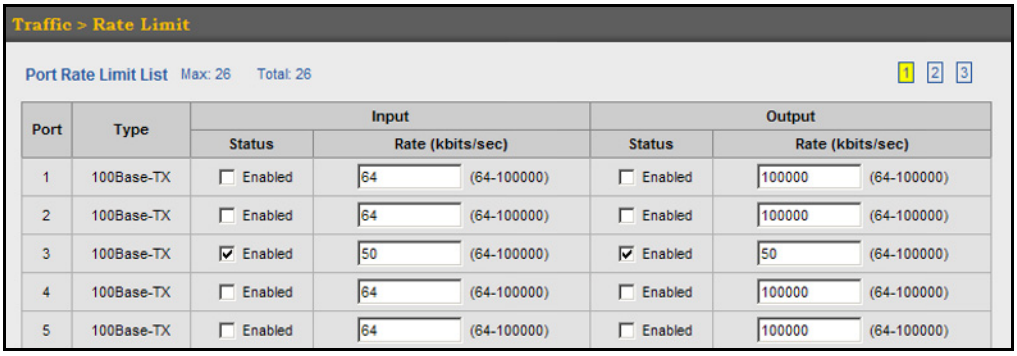
- **Port** – Displays the port number.
- **Type** – Indicates the port type. (100Base-TX, 1000Base-T, or SFP)
- **Status** – Enables or disables the rate limit. (Default: Disabled)
- **Rate** – Sets the rate limit level. (Range: 64 - 100,000 kbits per second for Fast Ethernet ports; 64 - 1,000,000 kbits per second for Gigabit Ethernet ports)

WEB INTERFACE

To configure rate limits:

1. Click Traffic, Rate Limit.
2. Enable the Rate Limit Status for the required ports.
3. Set the rate limit for the individual ports,.
4. Click Apply.

Figure 63: Configuring Rate Limits


Traffic > Rate Limit
Port Rate Limit List Max: 26 Total: 26
1 2 3
Port
Type
Input
Output
Status
Rate (kbits/sec)
Status
Rate (kbits/sec)
1 100Base-TX Enabled 64 (64-100000) Enabled 100000 (64-100000)
2 100Base-TX Enabled 64 (64-100000) Enabled 100000 (64-100000)
3 100Base-TX Enabled 50 (64-100000) Enabled 50 (64-100000)
4 100Base-TX Enabled 64 (64-100000) Enabled 100000 (64-100000)
5 100Base-TX Enabled 64 (64-100000) Enabled 100000 (64-100000)

10 STORM CONTROL CONFIGURATION

Use the Traffic > Storm Control page to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

COMMAND USAGE

- Storm Control is disabled by default.
- Broadcast control does not effect IP multicast traffic.
- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 Kbps, and the rate limit is set to 20000 Kbps on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.
- The description of effective rate limiting (see Command Usage under "Rate Limit Configuration" on page 119) also applies to storm control.

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.
- **Type** – Indicates interface type. (100Base-TX, 1000Base-T, or SFP)
- **Unknown Unicast** – Specifies storm control for unknown unicast traffic.
- **Multicast** – Specifies storm control for multicast traffic.
- **Broadcast** – Specifies storm control for broadcast traffic.
- **Status** – Enables or disables storm control. (Default: Disabled)

- **Rate** – Threshold level as a rate; i.e., kilobits per second. (Range: 64-100000 Kbps for Fast Ethernet ports, 64-1000000 Kbps for Gigabit Ethernet ports)

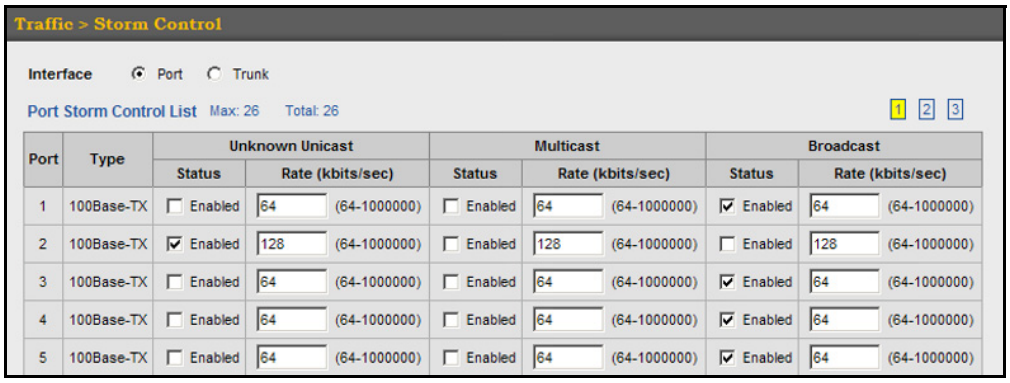
NOTE: Only one rate is supported for all traffic types on an interface.

WEB INTERFACE

To configure broadcast storm control:

1. Click Traffic, Storm Control.
2. Set the Status field to enable or disable storm control.
3. Set the required threshold beyond which the switch will start dropping packets.
4. Click Apply.

Figure 64: Configuring Storm Control


Traffic > Storm Control
Interface Port Trunk
Port Storm Control List Max: 26 Total: 26
1 2 3
Port Type Unknown Unicast Multicast Broadcast
Status Rate (kbits/sec) Status Rate (kbits/sec) Status Rate (kbits/sec)
1 100Base-TX Enabled 64 (64-1000000) Enabled 64 (64-1000000) Enabled 64 (64-1000000)
2 100Base-TX Enabled 128 (64-1000000) Enabled 128 (64-1000000) Enabled 128 (64-1000000)
3 100Base-TX Enabled 64 (64-1000000) Enabled 64 (64-1000000) Enabled 64 (64-1000000)
4 100Base-TX Enabled 64 (64-1000000) Enabled 64 (64-1000000) Enabled 64 (64-1000000)
5 100Base-TX Enabled 64 (64-1000000) Enabled 64 (64-1000000) Enabled 64 (64-1000000)

11 CLASS OF SERVICE

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

This chapter describes the following basic topics:

- Layer 2 Queue Settings – Configures each queue, including the default priority, queue mode, queue weight, and mapping of packets to queues based on CoS tags.
- Layer 3/4 Priority Settings – Selects the method by which inbound packets are processed (DSCP or CoS), and sets the per-hop behavior and drop precedence for internal processing.

LAYER 2 QUEUE SETTINGS

This section describes how to configure the default priority for untagged frames, set the queue mode, set the weights assigned to each queue, and map class of service tags to queues.

SETTING THE DEFAULT PRIORITY FOR INTERFACES

Use the Traffic > Priority > Default Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

COMMAND USAGE

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage, but can be configured to process each queue in strict order, or use a combination of strict and weighted queueing.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

PARAMETERS

These parameters are displayed:

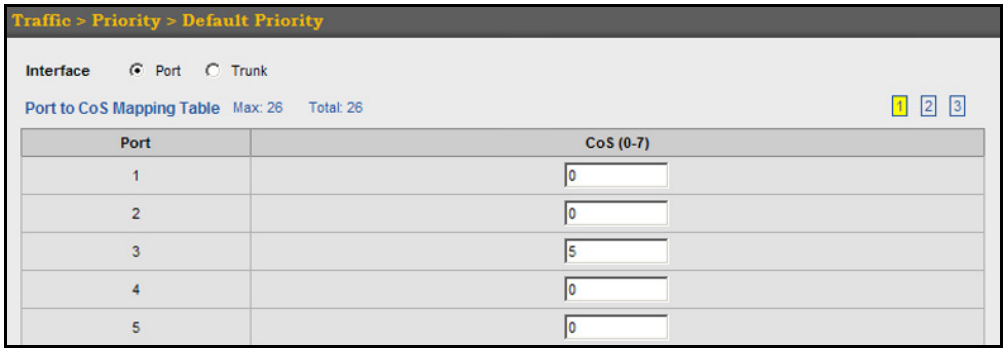
- **Interface** – Displays a list of ports or trunks.
- **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Default Priority.
2. Select the interface type to display (Port or Trunk).
3. Modify the default priority for any interface.
4. Click Apply.

Figure 65: Setting the Default Port Priority



SELECTING THE QUEUE MODE

Use the Traffic > Priority > Queue page to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, Shaped Deficit Weighted Round-Robin (SDWRR) queuing that specifies a scheduling weight for each queue. SDWRR is labelled WRR in the menu. It can also be configured to use a combination of strict and weighted queuing.

COMMAND USAGE

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- The WRR algorithm used by this switch is known as Shaped Deficit Weighted Round Robin (SDWRR).

The basic WRR algorithm uses a relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Deficit Weighted Round-Robin (DWRR) services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted. As a result, traffic on queues with large weights cause increased latency and jitter for traffic waiting for scheduling other queues. In SDWRR, if two or more queues have traffic eligible for transmission (i.e. the Deficit Counter is greater than the packet size to be transmitted), then a round-robin scheme among those queues is used, while still preserving the overall weight ratios between the queues. This produces less jitter and lower maximum latency for traffic on all of the serviced queues.

- If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.

- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

  Service time is shared at the egress ports by defining scheduling weights for SWDRR, or the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

- The specified queue mode applies to all interfaces.

PARAMETERS

These parameters are displayed:

- **Queue Mode**

  - **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

  - **WRR** (SWDRR) – Shares bandwidth at the egress ports by using scheduling weights, servicing each queue in a round-robin fashion.

  - **Strict and WRR** – Uses strict priority on the high-priority queues and SDWRR for the rest of the queues. (This is the default setting.)

- **Queue ID** – The ID of the priority queue. (Range: 0-7)

- **Strict Mode** – If "Strict and WRR" mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority when using the strict-weighted queuing mode. (Default: Strict and WRR mode, with Queue 3 using strict mode)

- **Weight** – Sets a weight for each queue which is used by the SDWRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6 are assigned to queues 0 - 3 respectively)

WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Queue.
2. Set the queue mode.
3. If the weighted queue mode is selected, the queue weight can be modified if required.
4. If the queue mode that uses a combination of strict and weighted queueing is selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.
5. Click Apply.

Figure 66: Setting the Queue Mode (Strict)

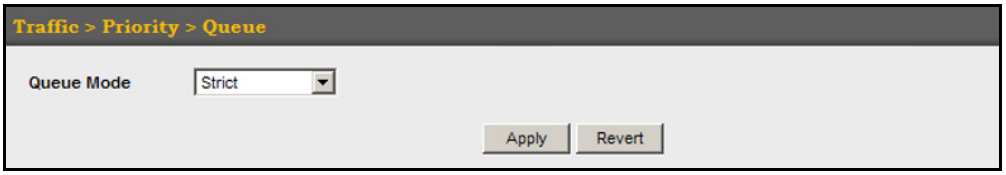


Figure 67: Setting the Queue Mode (WRR)

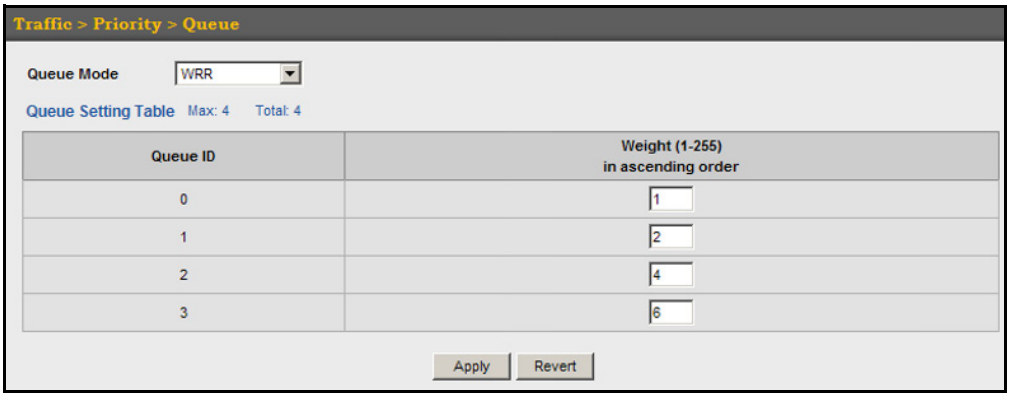
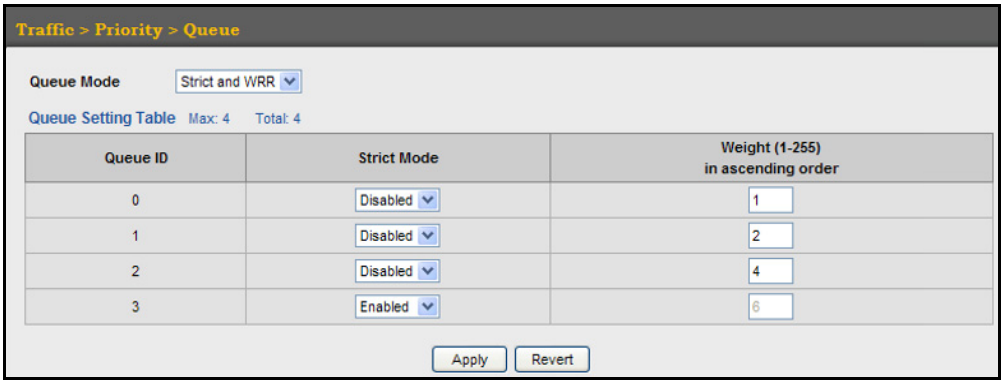


Figure 68: Setting the Queue Mode (Strict and WRR)



MAPPING COS VALUES TO EGRESS QUEUES

Use the Traffic > Priority > PHB to Queue page to specify the hardware output queues to use based on the internal per-hop behavior value. (For more information on exact manner in which the ingress priority tags are mapped to egress queues for internal processing, see "Mapping CoS Priorities to Internal DSCP Values" on page 136).

The switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on strict priority, Shaped Deficit Weighted Round-Robin (SDWRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in Table 12. This table indicates the default mapping of internal per-hop behavior to the hardware queues. The actual mapping may differ if the CoS priorities to internal DSCP values have been modified (page 136).

Table 12: IEEE 802.1p Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 13. However, priority levels can be mapped to the switch's output queues in any way that benefits application traffic for the network.

Table 13: CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

COMMAND USAGE

- Egress packets are placed into the hardware queues according to the mapping defined by this command.
- The default internal PHB to output queue mapping is shown below.

Table 14: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	1	0	0	1	2	2	3	3

- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

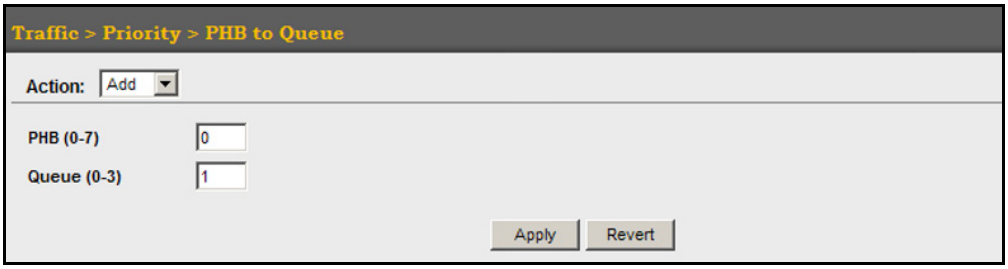
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7, where 7 is the highest priority)
- **Queue** – Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

WEB INTERFACE

To map internal PHB to hardware queues:

1. Click Traffic, Priority, PHB to Queue.
2. Select Add from the Action list.
3. Map an internal PHB to a hardware queue. Depending on how an ingress packet is processed internally based on its CoS value, and the assigned output queue, the mapping done on this page can effectively determine the service priority for different traffic classes.
4. Click Apply.

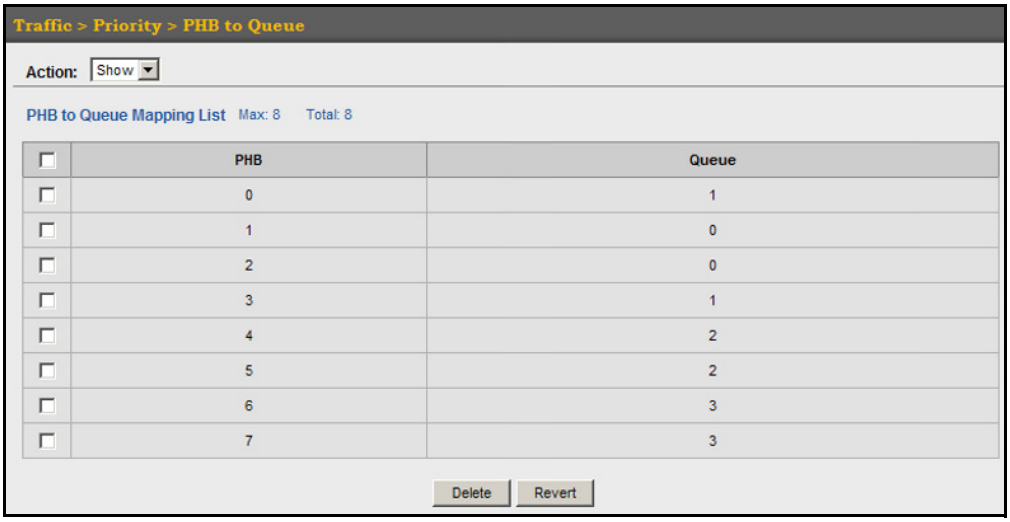
Figure 69: Mapping CoS Values to Egress Queues



To show the internal PHB to hardware queue map:

1. Click Traffic, Priority, PHB to Queue.
2. Select Show from the Action list.

Figure 70: Showing CoS Values to Egress Queue Mapping



LAYER 3/4 PRIORITY SETTINGS

Mapping Layer 3/4 Priorities to CoS Values

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet, or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner – The precedence for priority mapping is DSCP Priority and then Default Port Priority.

NOTE: The default settings used for mapping priority values from ingress traffic to internal DSCP values are used to determine the hardware queues used for egress traffic, not to replace the priority values. These defaults are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings, unless a queuing problem occurs with a particular application.

SETTING PRIORITY PROCESSING TO DSCP OR COS

The switch allows a choice between using DSCP or CoS priority processing methods. Use the Priority > Trust Mode page to select the required processing method.

COMMAND USAGE

- If the QoS mapping mode is set to DSCP, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see page 125) is used for priority processing.
- If the QoS mapping mode is set to CoS, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

  For an untagged packet, the default port priority (see page 125) is used for priority processing.

PARAMETERS

These parameters are displayed:

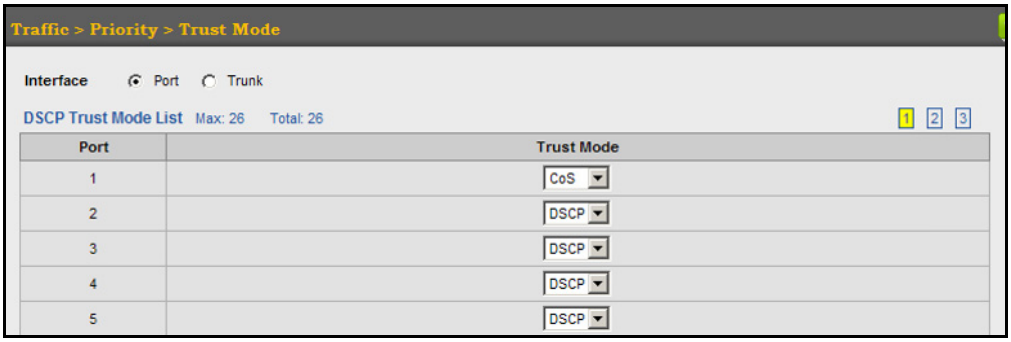
- **Interface** – Specifies a port or trunk.
- **Trust Mode**
  - **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values. (This is the default setting.)
  - **CoS** – Maps layer 3/4 priorities using Class of Service values.

WEB INTERFACE

To configure the trust mode:

1. Click Traffic, Priority, Trust Mode.
2. Select the interface type to display (Port or Trunk).
3. Set the trust mode.
4. Click Apply.

Figure 71: Setting the Trust Mode



MAPPING INGRESS DSCP VALUES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > DSCP to DSCP page to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

COMMAND USAGE

- Enter per-hop behavior and drop precedence for any of the DSCP values 0 - 63.

- This map is only used when the priority mapping mode is set to DSCP (see page 132), and the ingress packet type is IPv4.
- Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.
- Random Early Detection starts dropping yellow and red packets when the buffer fills up to 0x60 packets, and then starts dropping any packets regardless of color when the buffer fills up to 0x80 packets.
- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

- **DSCP** – DSCP value in ingress packets. (Range: 0-63)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 15: Default Mapping of DSCP Values to Internal PHB/Drop Values

ingress-dscp10 \ ingress-dscp1	0	1	2	3	4	5	6	7	8	9
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3.0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4.0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7.0	7,3
6	7,0	7,1	7,0	7,3						

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table.

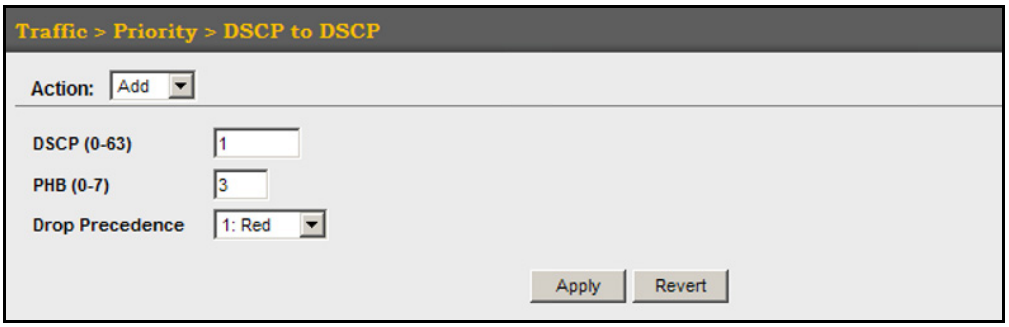
The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

WEB INTERFACE

To map DSCP values to internal PHB/drop precedence:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Add from the Action list.
3. Set the PHB and drop precedence for any DSCP value.
4. Click Apply.

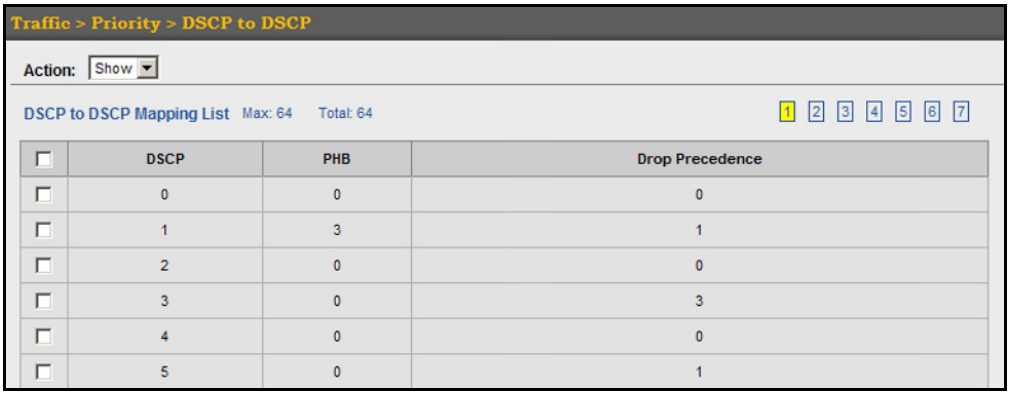
Figure 72: Configuring DSCP to DSCP Internal Mapping



To show the DSCP to internal PHB/drop precedence map:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Show from the Action list.

Figure 73: Showing DSCP to DSCP Internal Mapping



DSCP	PHB	Drop Precedence
0	0	0
1	3	1
2	0	0
3	0	3
4	0	0
5	0	1

MAPPING COS PRIORITIES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > CoS to DSCP page to maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

COMMAND USAGE

- The default mapping of CoS to PHB values is shown in Table 16 on page 137.
- Enter up to eight CoS/CFI paired values, per-hop behavior and drop precedence.
- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used by Random Early Detection (RED) to control traffic congestion.
- RED starts dropping yellow and red packets when the buffer fills up to 16 packets on Fast Ethernet ports and 72 packets on Gigabit Ethernet ports, and then starts dropping any packets regardless of color when the buffer fills up to 58 packets on Fast Ethernet ports and 80 packets on Gigabit Ethernet ports.
- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

- **CoS** – CoS value in ingress packets. (Range: 0-7)
- **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 16: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS	CFI 0	1
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

WEB INTERFACE

To map CoS/CFI values to internal PHB/drop precedence:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Add from the Action list.
3. Set the PHB and drop precedence for any of the CoS/CFI combinations.
4. Click Apply.

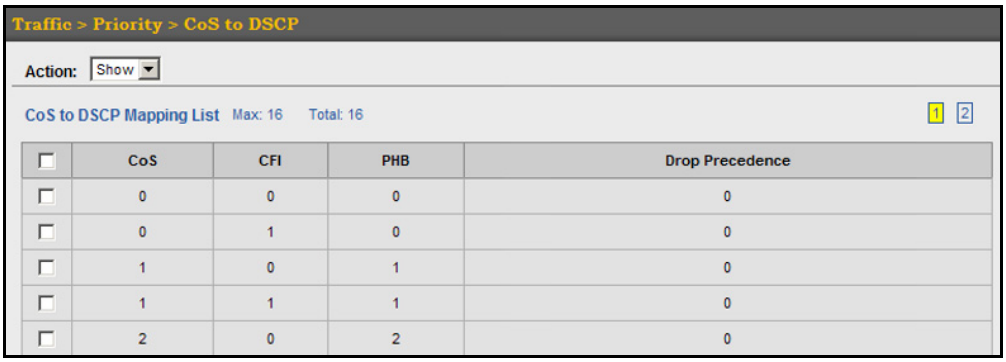
Figure 74: Configuring CoS to DSCP Internal Mapping



To show the CoS/CFI to internal PHB/drop precedence map:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Show from the Action list.
3. Select an interface.

Figure 75: Showing CoS to DSCP Internal Mapping


Traffic > Priority > CoS to DSCP
Action: Show
CoS to DSCP Mapping List Max: 16 Total: 16
1 2
CoS CFI PHB Drop Precedence
0 0 0 0
0 1 0 0
1 0 1 0
1 1 1 0
2 0 2 0

12 QUALITY OF SERVICE

This chapter describes the following tasks required to apply QoS policies:

Class Map – Creates a map which identifies a specific class of traffic.

Policy Map – Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic.

Binding to a Port – Applies a policy map to an ingress port.

OVERVIEW

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

NOTE: You can configure up to 16 rules per class map. You can also include multiple classes in a policy map.

NOTE: You should create a class map before creating a policy map. Otherwise, you will not be able to select a class map from the policy rule settings screen (see page 143).

COMMAND USAGE

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the Configure Class (Add) page to designate a class name for a specific category of traffic.
2. Use the Configure Class (Add Rule) page to edit the rules for each class which specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Use the Configure Policy (Add) page to designate a policy name for a specific manner in which ingress traffic will be handled.
4. Use the Configure Policy (Add Rule) page to add one or more classes to the policy map. Assign policy rules to each class by "setting" the QoS value (CoS or PHB) to be assigned to the matching traffic class. The policy rule can also be configured to monitor the maximum throughput and burst rate. Then specify the action to take for conforming traffic, or the action to take for a policy violation.
5. Use the Configure Interface page to assign a policy map to a specific interface.

CONFIGURING A CLASS MAP

A class map is used for matching packets to a specified class. Use the Traffic > DiffServ (Configure Class) page to configure a class map.

COMMAND USAGE

- The class map is used with a policy map (page 143) to create a service policy (page 153) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.
- Up to 32 class maps can be configured.

PARAMETERS

These parameters are displayed:

Add

- **Class Name** – Name of the class map. (Range: 1-16 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified on the Add page.
- **Description** – A brief description of a class map. (Range: 1-64 characters)

Add Rule

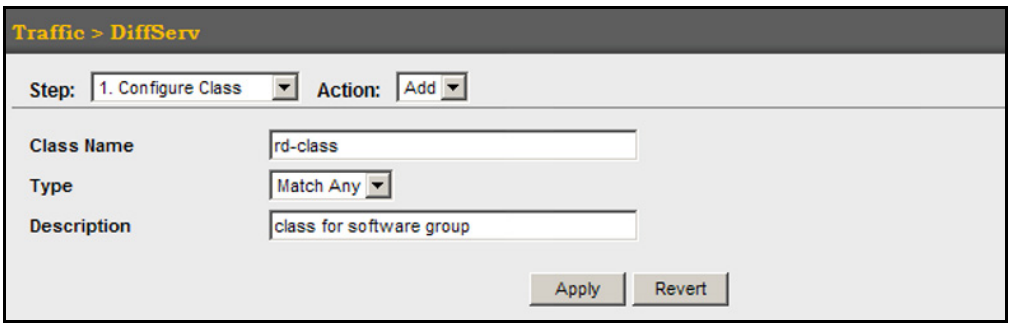
- **Class Name** – Name of the class map.
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **ACL** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN ID** – A VLAN. (Range:1-4093)

WEB INTERFACE

To configure a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add from the Action list.
4. Enter a class name.
5. Enter a description.
6. Click Add.

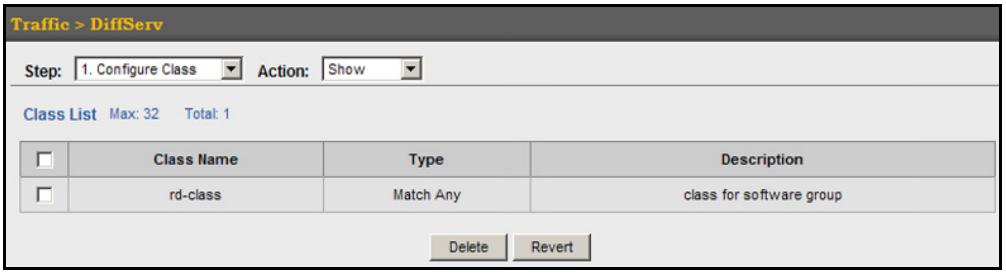
Figure 76: Configuring a Class Map



To show the configured class maps:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show from the Action list.

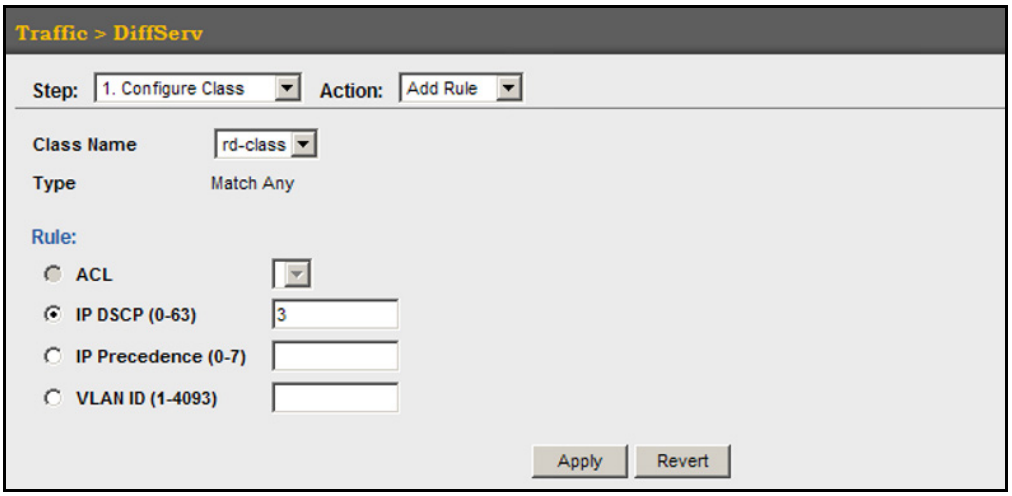
Figure 77: Showing Class Maps



To edit the rules for a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of a class map.
5. Specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN. You can specify up to 16 items to match when assigning ingress traffic to a class map.
6. Click Apply.

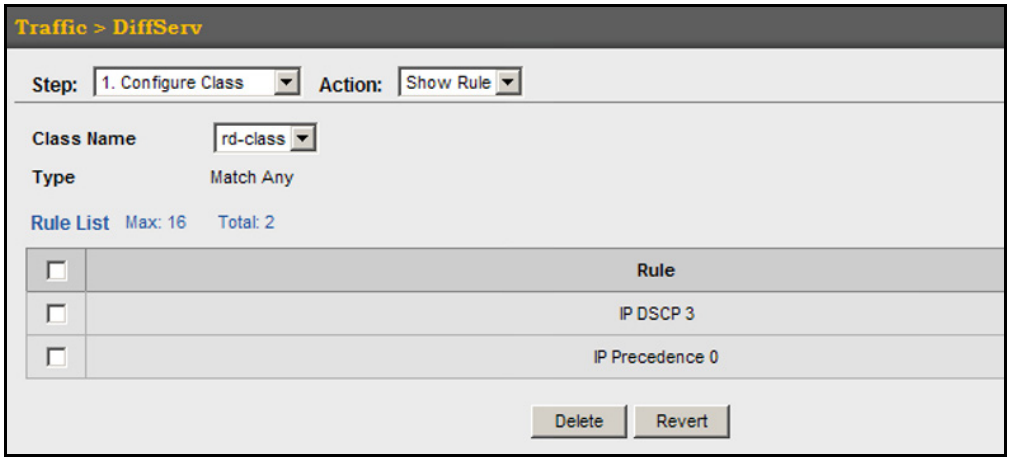
Figure 78: Adding Rules to a Class Map



To show the rules for a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show Rule from the Action list.

Figure 79: Showing the Rules for a Class Map



CREATING QOS POLICIES

Use the Traffic > DiffServ (Configure Policy) page to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements (page 140), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces (page 153).

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps.

The class of service or per-hop behavior (i.e., the priority used for internal queue processing) can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to conforming and non-conforming traffic based by one of three distinct policing methods as described below.

Police Flow Meter – Defines the committed information rate (maximum throughput), committed burst size (burst rate), and the action to take for conforming and non-conforming traffic.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the "burst" field (BC), and the average rate tokens are removed from the bucket is specified by the "rate" option (CIR). Action may be taken for traffic conforming to the maximum throughput, or exceeding the maximum throughput.

srTCM Police Meter – Defines an enforcer for classified traffic based on a single rate three color meter scheme defined in RFC 2697. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and excess burst size (BE). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the excess burst size.

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection. A packet is marked green if it doesn't exceed the committed information rate and committed burst size, yellow if it does exceed the committed information rate and committed burst size, but not the excess burst size, and red otherwise.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

  The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - if Te is less then BE, Te is incremented by one, else
  - neither Tc nor Te is incremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Blind mode:

  - If $Tc(t)-B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else

- if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0,
- else the packet is red and neither Tc nor Te is decremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as green and Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else
- the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

trTCM Police Meter – Defines an enforcer for classified traffic based on a two rate three color meter scheme defined in RFC 2698. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate), and peak burst size (BP). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the peak burst size.

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

  The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR,

respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.

The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Blind mode:

- If Tp(t)-B < 0, the packet is red, else
- if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as red or if Tp(t)-B < 0, the packet is red, else
- if the packet has been precolored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

- The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

Random Early Detection – RED starts dropping yellow and red packets when the buffer fills up to 0x60 packets, and then starts dropping any packets regardless of color when the buffer fills up to 0x80 packets.

COMMAND USAGE

- A policy map can contain 128 class statements that can be applied to the same interface (page 153). Up to 32 policy maps can be configured for ingress ports.

- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 153) to take effect.

PARAMETERS

These parameters are displayed:

Add

- **Policy Name** – Name of policy map. (Range: 1-16 characters)
- **Description** – A brief description of a policy map. (Range: 1-256 characters)

Add Rule

- **Policy Name** – Name of policy map.
- **Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.
- **Action –** This attribute is used to set an internal QoS value in hardware for matching packets. The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.
  - **Set CoS** – Configures the service provided to ingress traffic by setting an internal CoS value for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

    See Table 16, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence," on page 137).
  - **Set PHB** – Configures the service provided to ingress traffic by setting the internal per-hop behavior for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

    See Table 15, "Default Mapping of DSCP Values to Internal PHB/Drop Values," on page 134).
  - **Set IP DSCP** – Configures the service provided to ingress traffic by setting an IP DSCP value for a matching packet (as specified in rule settings for a class map). (Range: 0-63)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
- **Meter Mode** – Selects one of the following policing methods.
  - **Flow** (Police Flow) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and the action to take for conforming and non-conforming traffic. Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the "burst" field, and the average rate tokens are removed from the bucket is by specified by the "rate" option.

- **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

  The rate cannot exceed the configured interface speed.

- **Committed Burst Size** (BC) – Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

  - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

- **Violate** – Specifies whether the traffic that exceeds the maximum rate (CIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

  - **Drop** – Drops out of conformance traffic.

- **srTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate) and excess burst size (BE), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the excess burst size, or exceeding the excess burst size. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection.

  The color modes include "Color-Blind" which assumes that the packet stream is uncolored, and "Color-Aware" which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under "srTCM Police Meter."

  - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

  - **Committed Burst Size** (BC) – Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Exceeded Burst Size** (BE) – Burst in excess of committed burst size. (Range: 4000-16000000 at a granularity of 4k bytes)

The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.
  - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.
- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.
  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
  - **Drop** – Drops out of conformance traffic.
- **Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.
  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
  - **Drop** – Drops out of conformance traffic.

- **trTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate) and peak burst size (BP), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the peak information rate, or exceeding the peak information rate. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection.

  The color modes include "Color-Blind" which assumes that the packet stream is uncolored, and "Color-Aware" which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under "trTCM Police Meter."

  - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.
  - **Peak Information Rate** (PIR) – Rate in kilobits per second. (Range: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

- **Committed Burst Size** (BC) – Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

- **Peak Burst Size** (BP) – Burst size in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

  - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

  - **Drop** – Drops out of conformance traffic.

- **Violate** – Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

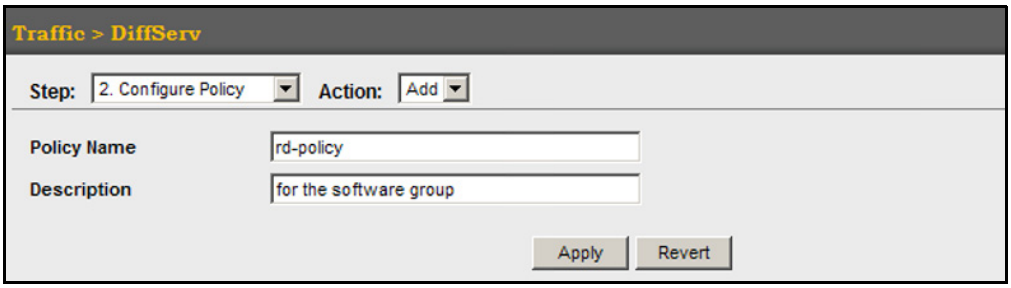
  - **Drop** – Drops out of conformance traffic.

WEB INTERFACE

To configure a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Add from the Action list.
4. Enter a policy name.
5. Enter a description.
6. Click Add.

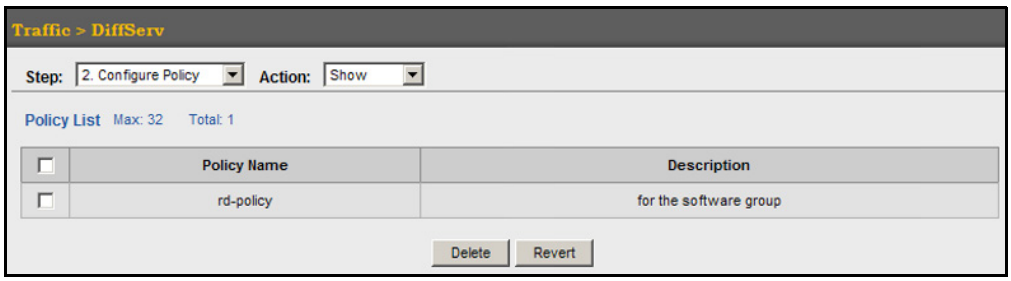
Figure 80: Configuring a Policy Map



To show the configured policy maps:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Show from the Action list.

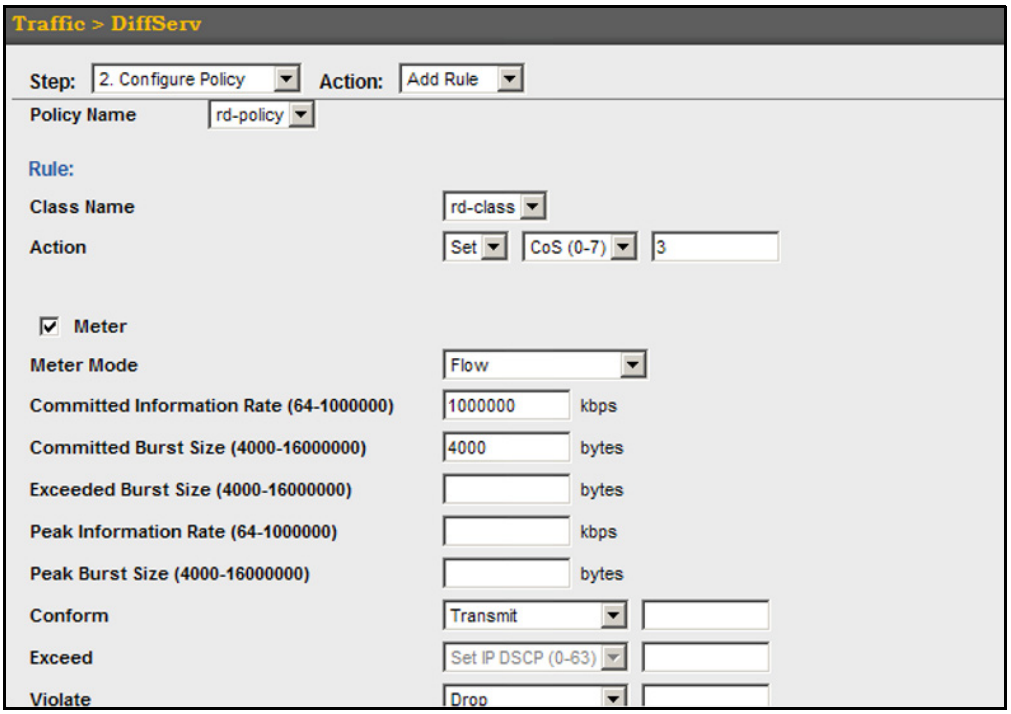
Figure 81: Showing Policy Maps



To edit the rules for a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of a policy map.
5. Set the CoS or per-hop behavior for matching packets to specify the quality of service to be assigned to the matching traffic class. Use one of the metering options to define parameters such as the maximum throughput and burst rate. Then specify the action to take for conforming traffic, the action to tack for traffic in excess of the maximum rate but within the peak information rate, or the action to take for a policy violation.
6. Click Apply.

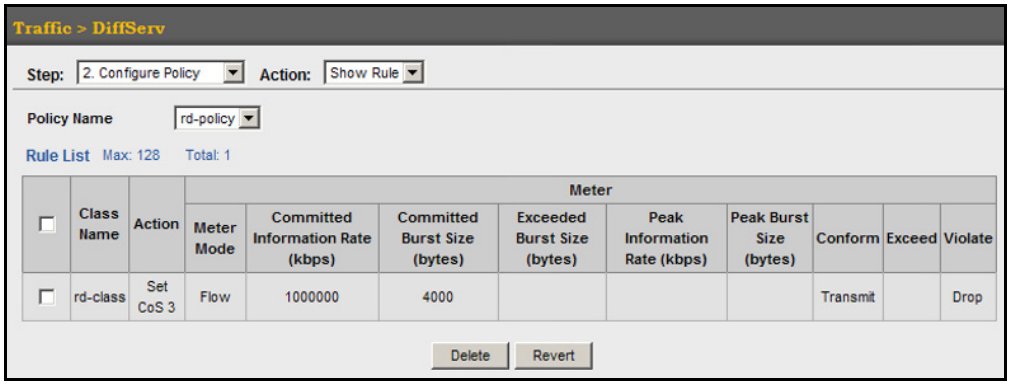
Figure 82: Adding Rules to a Policy Map



To show the rules for a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Show Rule from the Action list.

Figure 83: Showing the Rules for a Policy Map



ATTACHING A POLICY MAP TO A PORT

Use the Traffic > DiffServ (Configure Interface) page to bind a policy map to an ingress port.

COMMAND USAGE

- First define a class map, define a policy map, and bind the service policy to the required interface.
- Only one policy map can be bound to an interface.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

PARAMETERS

These parameters are displayed:

- **Port** – Specifies a port.
- **Ingress** – Applies the selected rule to ingress traffic.

WEB INTERFACE

To bind a policy map to a port:

1. Click Traffic, DiffServ.
2. Select Configure Interface from the Step list.
3. Check the box under the Ingress field to enable a policy map for a port.
4. Select a policy map from the scroll-down box.
5. Click Apply.

Figure 84: Attaching a Policy Map to a Port



13 VoIP Traffic Configuration

This chapter covers the following topics:

- Global Settings – Enables VOIP globally, sets the Voice VLAN, and the aging time for attached ports.
- Telephony OUI List – Configures the list of phones to be treated as VOIP devices based on the specified Organization Unit Identifier (OUI).
- Port Settings – Configures the way in which a port is added to the Voice VLAN, the filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to voice traffic.

Overview

When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation can provide higher voice quality by preventing excessive packet delays, packet loss, and jitter. This is best achieved by assigning all VoIP traffic to a single Voice VLAN.

The use of a Voice VLAN has several advantages. It provides security by isolating the VoIP traffic from other data traffic. End-to-end QoS policies and high priority can be applied to VoIP VLAN traffic across the network, guaranteeing the bandwidth it needs. VLAN isolation also protects against disruptive broadcast and multicast traffic that can seriously affect voice quality.

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. The VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member the Voice VLAN. Alternatively, switch ports can be manually configured.

Configuring VoIP Traffic

Use the Traffic > VoIP (Configure Global) page to configure the switch for VoIP traffic. First enable automatic detection of VoIP devices attached to the switch ports, then set the Voice VLAN ID for the network. The Voice VLAN aging time can also be set to remove a port from the Voice VLAN when VoIP traffic is no longer received on the port.

COMMAND USAGE

All ports are set to VLAN access mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first set the VLAN membership mode to hybrid (see "Adding Static Members to VLANs" on page 96).

PARAMETERS

These parameters are displayed:

- **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- **Voice VLAN** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4093)
- **Voice VLAN Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

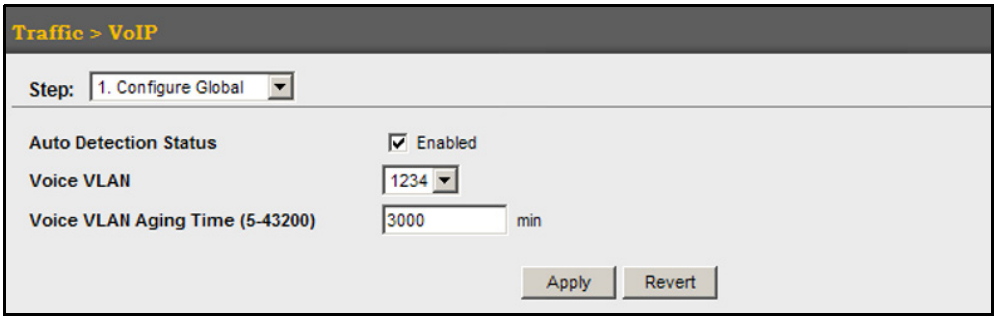
NOTE: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

WEB INTERFACE

To configure global settings for a Voice VLAN:

1. Click Traffic, VoIP.
2. Select Configure Global from the Step list.
3. Enable Auto Detection.
4. Specify the Voice VLAN ID.
5. Adjust the Voice VLAN Aging Time if required.
6. Click Apply.

Figure 85: Configuring a Voice VLAN



CONFIGURING TELEPHONY OUI

VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP. Use the Traffic > VoIP (Configure OUI) page to configure this feature.

PARAMETERS

These parameters are displayed:

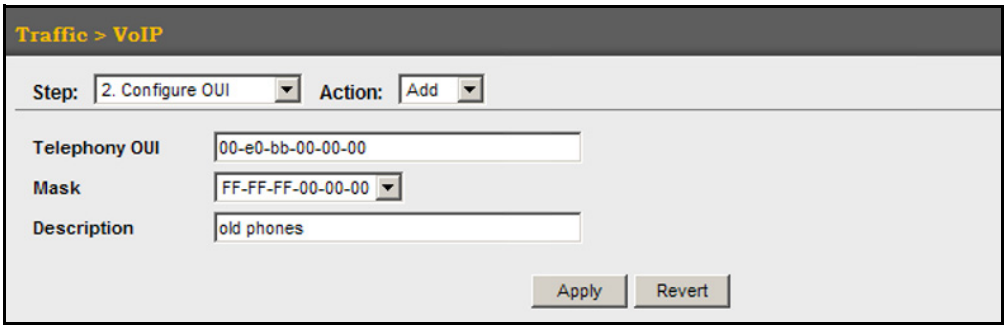
- **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- **Mask** – Identifies a range of MAC addresses. Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address.
  (Default: FF-FF-FF-00-00-00)
- **Description** – User-defined text that identifies the VoIP devices.

WEB INTERFACE

To configure MAC OUI numbers for VoIP equipment:

1. Click Traffic, VoIP.
2. Select Configure OUI from the Step list.
3. Select Add from the Action list.
4. Enter a MAC address that specifies the OUI for VoIP devices in the network.
5. Select a mask from the pull-down list to define a MAC address range.
6. Enter a description for the devices.
7. Click Apply.

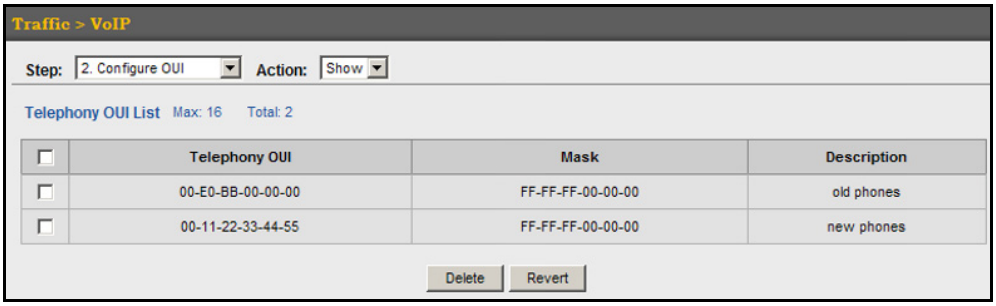
Figure 86: Configuring an OUI Telephony List



To show the MAC OUI numbers used for VoIP equipment:

1. Click Traffic, VoIP.
2. Select Configure OUI from the Step list.
3. Select Show from the Action list.

Figure 87: Showing an OUI Telephony List



CONFIGURING VOIP TRAFFIC PORTS

Use the Traffic > VoIP (Configure Interface) page to configure ports for VoIP traffic, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only VoIP traffic is forwarded on the Voice VLAN.

COMMAND USAGE

All ports are set to VLAN access mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first set the VLAN membership mode to hybrid (see "Adding Static Members to VLANs" on page 96).

PARAMETERS

These parameters are displayed:

- **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)

- **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.
- **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1ab (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.
- **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

- **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)

- **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
  - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
  - **LLDP** – Uses LLDP (IEEE 802.1AB) to discover VoIP devices attached to the port. LLDP checks that the "telephone bit" in the system capability TLV is turned on. See "Link Layer Discovery Protocol" on page 205 for more information on LLDP.

- **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)

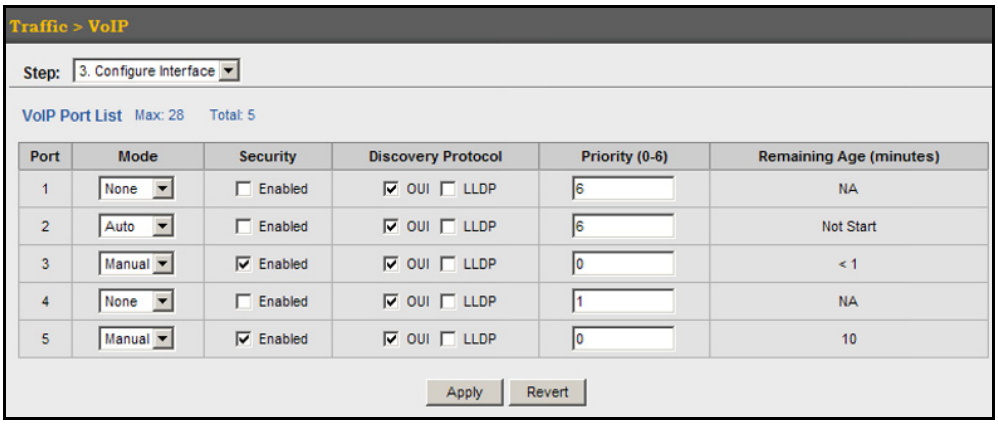
- **Remaining Age** – Number of minutes before this entry is aged out.

WEB INTERFACE

To configure VoIP traffic settings for a port:

1. Click Traffic, VoIP.
2. Select Configure Interface from the Step list.
3. Configure any required changes to the VoIP settings each port.
4. Click Apply.

Figure 88: Configuring Port Settings for a Voice VLAN



14 SECURITY MEASURES

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access to the data ports. This switch provides secure network management access using the following options:

- AAA – Use local or remote authentication to specify authentication servers.
- User Accounts – Manually configure access rights on the switch for specified users.
- Network Access - Configure secure MAC address aging and dynamic VLAN assignment.
- HTTPS – Provide a secure web connection.
- ACL – Access Control Lists provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code).
- IP Filter – Filters management access to the web or SNMP interface.
- Port Security – Configure secure addresses for individual ports.
- Port Authentication – Use IEEE 802.1X port authentication to control access to specific ports.



NOTE: The priority of execution for the filtering commands is Port Security, Port Authentication, Network Access, and then Access Control Lists.

CONFIGURING LOCAL/REMOTE LOGON AUTHENTICATION

Use the Security > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

COMMAND USAGE

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence. Then specify the corresponding parameters for the remote authentication protocol using the Security > AAA > Server page. Local and remote logon authentication control management access via a web browser.

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

PARAMETERS

These parameters are displayed:

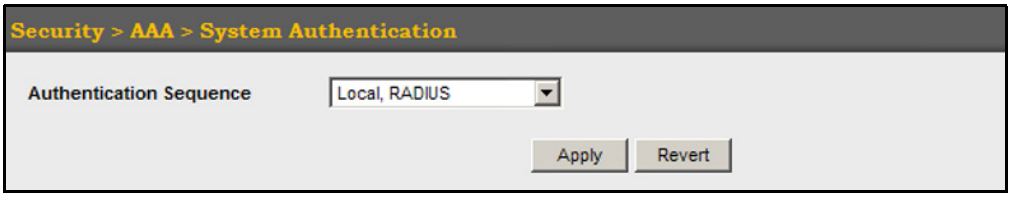
- **Authentication Sequence** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **RADIUS** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

WEB INTERFACE

To configure the method(s) of controlling management access:

1. Click Security, AAA, System Authentication.
2. Specify the authentication sequence (i.e., one to three methods).
3. Click Apply.

Figure 89: Configuring the Authentication Sequence

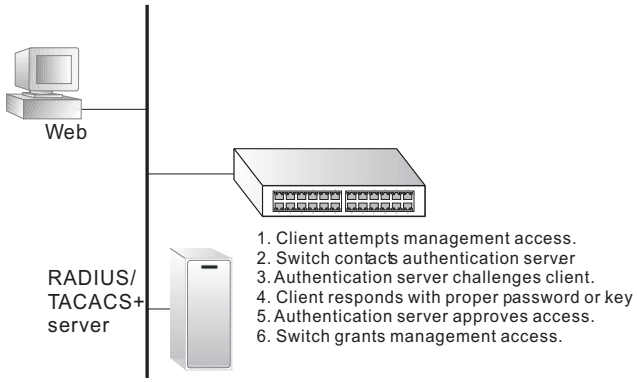


CONFIGURING REMOTE LOGON AUTHENTICATION SERVERS

Use the Security > AAA > Server page to configure the message exchange parameters for RADIUS or TACACS+ remote access authentication servers.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

Figure 90: Authentication Server Operation



RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

COMMAND USAGE

- If a remote authentication server is used, you must specify the message exchange parameters for the remote authentication protocol. Both local and remote logon authentication control management access via the web browser.

- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the

server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

PARAMETERS

These parameters are displayed:

- **RADIUS**
  - **Global** – Provides globally applicable RADIUS settings.
  - **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
  - **Server IP Address** – Address of authentication server. (A Server Index entry must be selected to display this item.)
  - **Authentication Server UDP Port** – Network (UDP) port on authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
  - **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
  - **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
  - **Set Key** – Mark this box to set or modify the encryption key.
  - **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
  - **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.
- **TACACS+**
  - **Global** – Provides globally applicable TACACS+ settings.
  - **Server Index** – Specifies the index number of the server to be configured. The switch currently supports only one TACACS+ server.
  - **Server IP Address** – Address of the TACACS+ server. (A Server Index entry must be selected to display this item.)
  - **Authentication Server TCP Port** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)

- **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
- **Set Key** – Mark this box to set or modify the encryption key.
- **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

WEB INTERFACE

To configure the parameters for RADIUS or TACACS+ authentication:

1. Click Security, AAA, Server.
2. Select RADIUS or TACACS+ server type.
3. Select Global to specify the parameters that apply globally to all specified servers, or select a specific Server Index to specify the parameters that apply to a specific server.
4. To set or modify the authentication key, mark the Set Key box, enter the key, and then confirm it
5. Click Apply.

Figure 91: Configuring Remote Authentication Server (RADIUS)

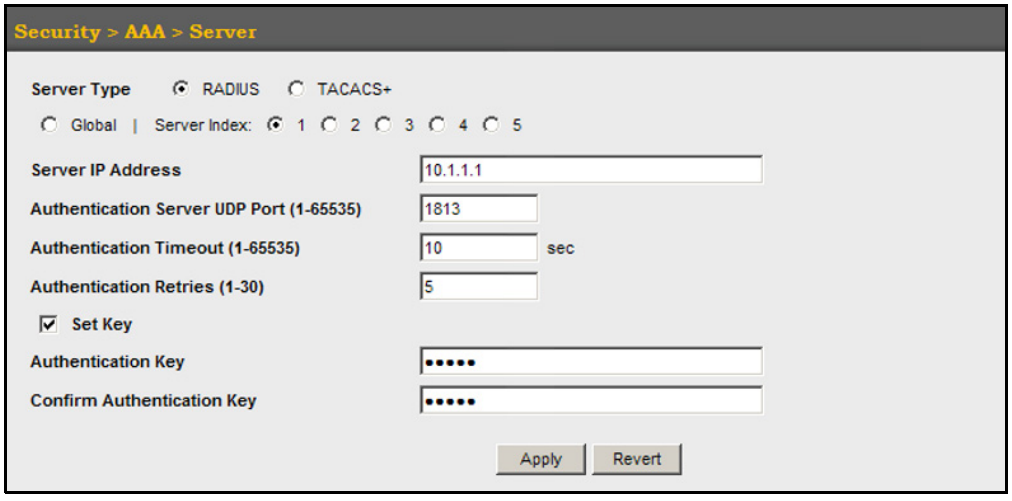
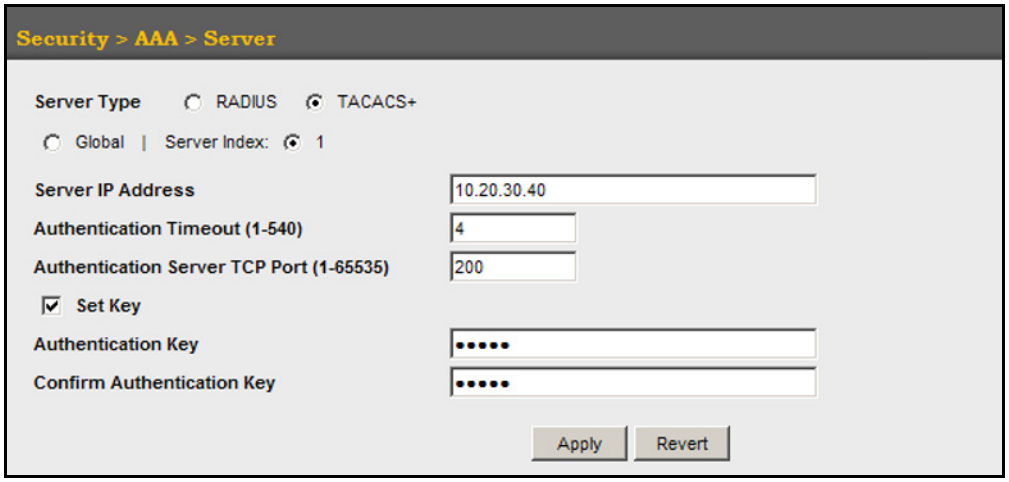


Figure 92: Configuring Remote Authentication Server (TACACS+)



CONFIGURING USER ACCOUNTS

Use the Security > User Accounts page to control management access to the switch based on manually configured user names and passwords.

COMMAND USAGE

- The default guest name is "guest" with the password "guest." The default administrator name is "admin" with the password "admin."
- The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

PARAMETERS

These parameters are displayed:

- **User Name** – The name of the user.
  (Maximum length: 8 characters; maximum number of users: 16)
- **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged)

  Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.
- **Password Type** – Plain Text or Encrypted password.

  The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP or FTP server. There is no need for you to manually configure encrypted passwords.

- **Password** – Specifies the user password.
(Range: 0-8 characters plain text, 32 encrypted, case sensitive)

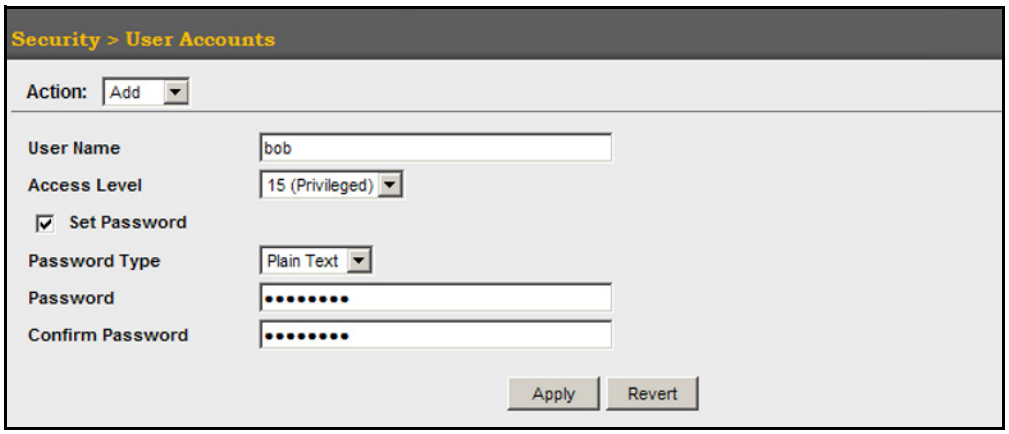
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

WEB INTERFACE

To configure user accounts:

1. Click Security, User Accounts.
2. Select Add from the Action list.
3. Specify a user name, select the user's access level, then enter a password if required and confirm it.
4. Click Apply.

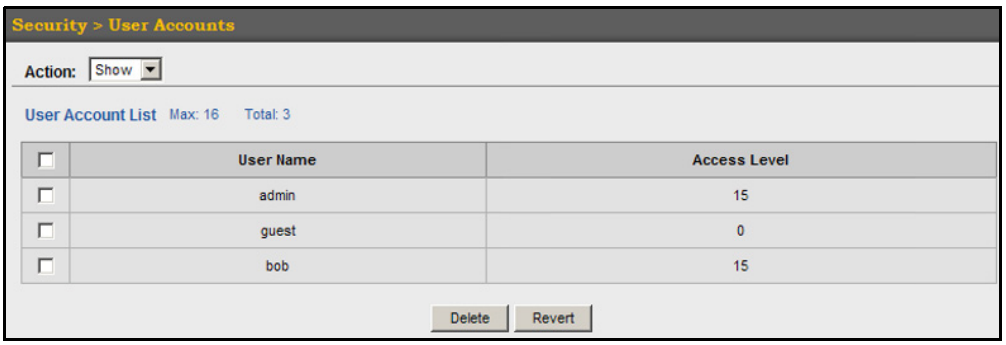
Figure 93: Configuring User Accounts



To show user accounts:

1. Click Security, User Accounts.
2. Select Show from the Action list.

Figure 94: Showing User Accounts



NETWORK ACCESS

The Network Access pages are used to enable aging for secure addresses stored in the MAC address table (using 802.1X), and to assign a host to the VLANs specified for that specific device on a RADIUS server (see "Configuring 802.1X Port Authentication" on page 189).

COMMAND USAGE

- When Dynamic VLAN is enabled on a port, the 802.1X authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The type of user name and password sent to the RADIUS server depends on 802.1X Operation Mode (page 192). Text is used for normal host-based authentication, or the host's MAC address is used for both the user name and password for MAC-based authentication. When MAC-based authentication is used by 802.1X, the PAP user name and password on the RADIUS server must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).

- If the RADIUS server finds an entry for the host, and that entry contains a VLAN identifier list, this list will be returned to the switch and applied to the port. The following attributes need to be configured on the RADIUS server.

  - **Tunnel-Type** = VLAN
  - **Tunnel-Medium-Type** = 802
  - **Tunnel-Private-Group-ID** = 1u,2t [*VLAN ID list*]

  The VLAN identifier list is carried in the RADIUS "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t,3u" where "u" indicates an untagged VLAN and "t" a tagged VLAN.

CONFIGURING GLOBAL SETTINGS FOR NETWORK ACCESS

Use the Security > Network Access (Configure Global) page to enable aging for secure addresses stored in the MAC address table (see "Configuring 802.1X Port Authentication" on page 189).

PARAMETERS

These parameters are displayed:

- **Aging Status** – Enables aging for dynamically learned secure addresses stored in the MAC address table. (Default: Disabled)

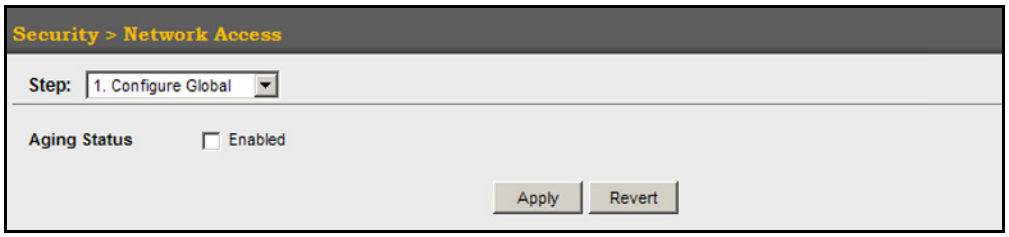
  This parameter applies to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 192).

WEB INTERFACE

To configure aging status for secure addresses stored in the MAC address table by 802.1X:

1. Click Security, Network Access.
2. Select Configure Global from the Step list.
3. Enable or disable aging for secure addresses.
4. Click Apply.

Figure 95: Configuring Global Settings for Network Access



CONFIGURING NETWORK ACCESS FOR PORTS

Use the Security > Network Access (Configure Interface) page to enable dynamic VLAN assignments.

PARAMETERS

These parameters are displayed:

- **Dynamic VLAN** – Enables dynamic VLAN assignment for a port. When enabled, any VLAN identifiers returned by the RADIUS server through the 802.1X authentication process are applied to the port, providing the VLANs have already been created on the switch. (GVRP is not used to create the VLANs.) (Default: Enabled)

  The VLAN settings specified by the first authenticated MAC address (using the 802.1X authentication process) are implemented for a port. Other authenticated MAC addresses on the port must have the same VLAN configuration, otherwise they are treated as authentication failures.

  If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration (to the 802.1X authentication process), the authentication is still treated as a success, and the host is assigned to the default untagged VLAN.

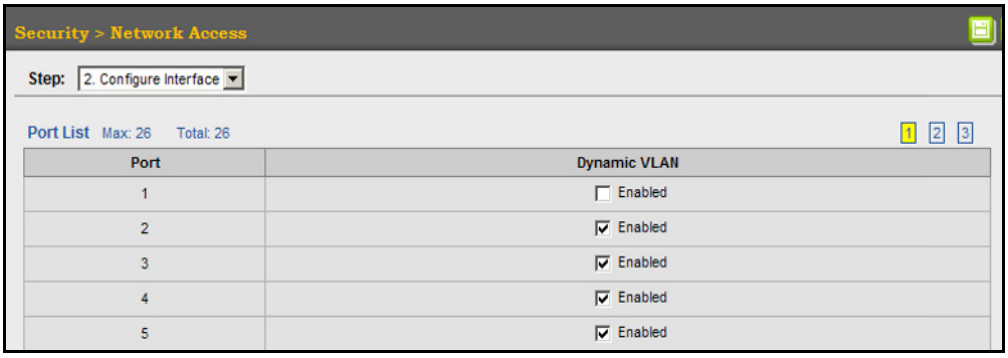
  When the dynamic VLAN assignment status is changed on a port, all authenticated addresses mapped to that port are cleared from the secure MAC address table.

WEB INTERFACE

To configure dynamic VLAN assignment on switch ports:

1. Click Security, Network Access.
2. Select Configure Interface from the Step list.
3. Set the dynamic VLAN status.
4. Click Apply.

Figure 96: Configuring Interface Settings for Network Access



DISPLAYING SECURE MAC ADDRESS INFORMATION

Use the Security > Network Access (Show Information) page to display the authenticated MAC addresses stored in the secure MAC address table. Information on the secure MAC entries can be displayed and selected entries can be removed from the table.

PARAMETERS

These parameters are displayed:

- **Query By** – Specifies parameters to use in the MAC address query.
  - **Sort Key** – Sorts the information displayed based on MAC address, port interface, or attribute.
  - **MAC Address** – Specifies a specific MAC address.
  - **Interface** – Specifies a port interface.
  - **Attribute** – Displays static or dynamic addresses.
- **Authenticated MAC Address List**
  - **MAC Address** – The authenticated MAC address.
  - **Interface** – The port interface associated with a secure MAC address.
  - **RADIUS Server** – The IP address of the RADIUS server that authenticated the MAC address.

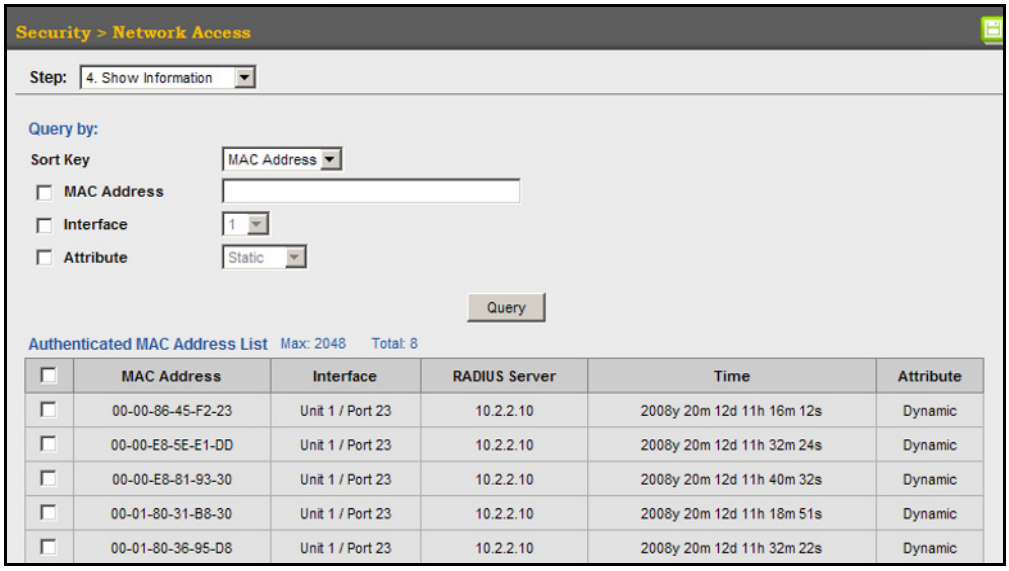
- **Time** – The time when the MAC address was last authenticated.
- **Attribute** – Indicates a static or dynamic address.

WEB INTERFACE

To display the authenticated MAC addresses stored in the secure MAC address table:

1. Click Security, Network Access.
2. Select Show Information from the Step list.
3. Use the sort key to display addresses based MAC address, interface, or attribute.
4. Restrict the displayed addresses by entering a specific address in the MAC Address field, specifying a port in the Interface field, or setting the address type to static or dynamic in the Attribute field.
5. Click Query.

Figure 97: Showing Addresses Authenticated for Network Access



CONFIGURING HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

CONFIGURING GLOBAL SETTINGS FOR HTTPS

Use the Security > HTTPS (Configure Global) page to enable or disable HTTPS and specify the UDP port used for this service.

COMMAND USAGE

- HTTP and HTTPS are implemented as mutually exclusive services on the switch. If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.
- The following web browsers and operating systems currently support HTTPS:

Table 17: HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 173.

NOTE: Users are automatically logged off of the HTTP server or HTTPS server if no input is detected for 600 seconds.

PARAMETERS

These parameters are displayed:

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Disabled)
- **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

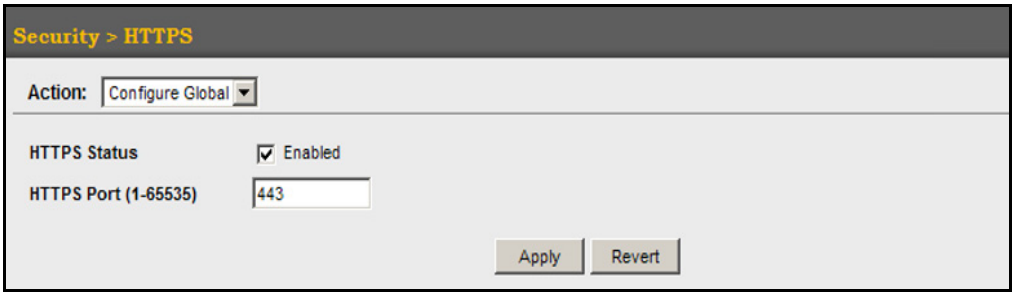
  The HTTPS port number cannot be set to 80.

WEB INTERFACE

To configure HTTPS:

1. Click Security, HTTPS.
2. Select Configure Global from the Step list.
3. Enable HTTPS and specify the port number if required.
4. Click Apply.

Figure 98: Configuring HTTPS



REPLACING THE DEFAULT SECURE-SITE CERTIFICATE

Use the Security > HTTPS (Copy Certificate) page to replace the default secure-site certificate.

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

CAUTION: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server and transfer them to the switch to replace the default (unrecognized) certificate with an authorized one.

NOTE: The switch must be reset for the new certificate to be activated. To reset the switch, see "Resetting the System" on page 63.

PARAMETERS

These parameters are displayed:

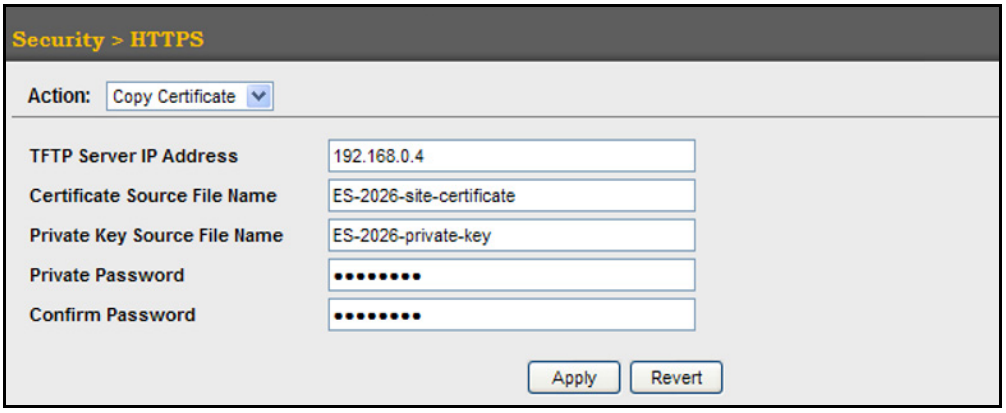
- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Certificate Source File Name** – Name of certificate file stored on the TFTP server.
- **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

WEB INTERFACE

To replace the default secure-site certificate:

1. Click Security, HTTPS.
2. Select Copy Certificate from the Step list.
3. Fill in the TFTP server, certificate and private key file name, and private password.
4. Click Apply.

Figure 99: Downloading the Secure-Site Certificate



ACCESS CONTROL LISTS

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists –

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

COMMAND USAGE

The following restrictions apply to ACLs:

- The maximum number of ACLs is 64.
- The maximum number of rules per system is 512 rules.
- An ACL can have up to 32 rules. However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.

SHOWING TCAM UTILIZATION

Use the Security > ACL (Configure ACL - Show TCAM) page to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

PARAMETERS

These parameters are displayed:

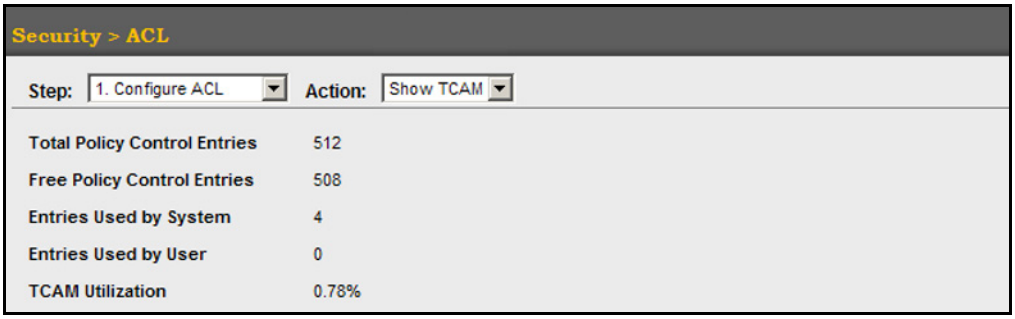
- **Total Policy Control Entries** – The number policy control entries in use.
- **Free Policy Control Entries** – The number of policy control entries available for use.
- **Entries Used by System** – The number of policy control entries used by the operating system.
- **Entries Used by User** – The number of policy control entries used by configuration settings, such as access control lists.
- **TCAM Utilization** – The overall percentage of TCAM in use.

WEB INTERFACE

To show information on TCAM utilization:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show TCAM from the Action list.

Figure 100: Showing TCAM Utilization


Security > ACL
Step: 1. Configure ACL
Action: Show TCAM
Total Policy Control Entries 512
Free Policy Control Entries 508
Entries Used by System 4
Entries Used by User 0
TCAM Utilization 0.78%

SETTING THE ACL NAME AND TYPE

Use the Security > ACL (Configure ACL - Add) page to create an ACL.

PARAMETERS

These parameters are displayed:

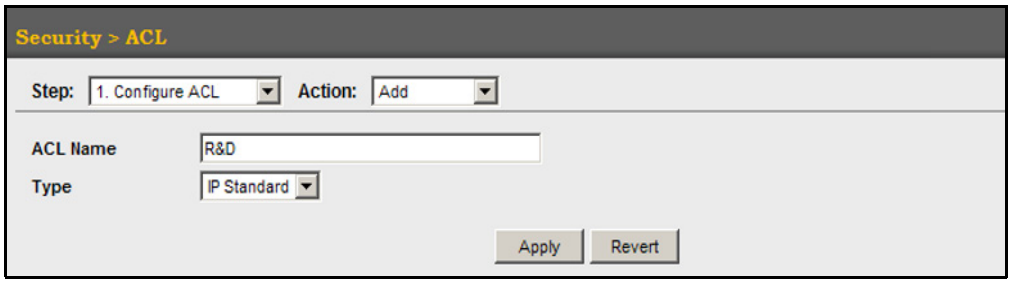
- **ACL Name** – Name of the ACL. (Maximum length: 15 characters)
- **Type** – The following filter modes are supported:
  - **IP Standard**: IPv4 ACL mode filters packets based on the source IPv4 address.
  - **IP Extended**: IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the "TCP" protocol is specified, then you can also filter packets based on the TCP control code.
  - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

WEB INTERFACE

To configure the name and type of an ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add from the Action list.
4. Fill in the ACL Name field, and select the ACL type.
5. Click Apply.

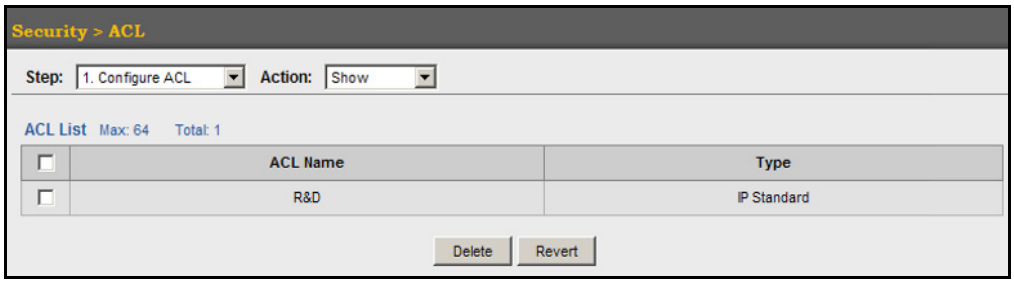
Figure 101: Creating an ACL



To show a list of ACLs:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show from the Action list.

Figure 102: Showing a List of ACLs



CONFIGURING A STANDARD IPV4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Standard) page to configure a Standard IPv4 ACL.

PARAMETERS

These parameters are displayed:

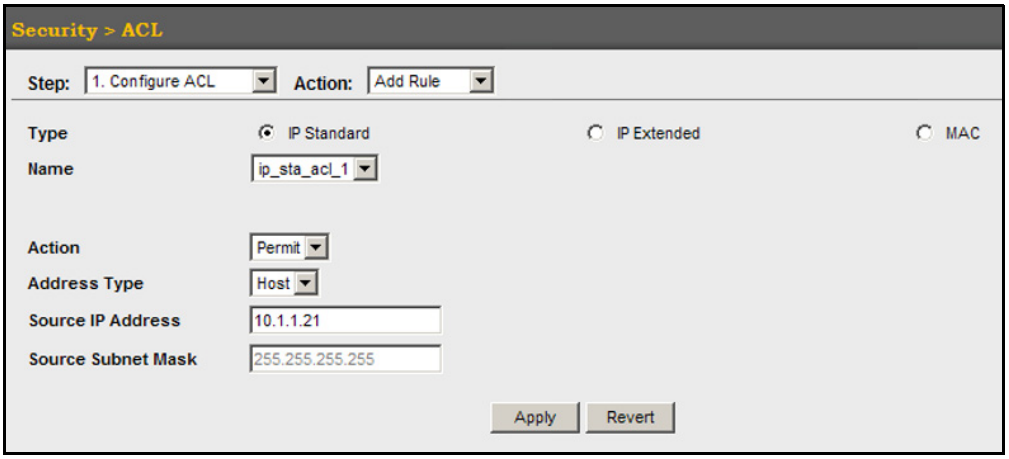
- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **Source IP Address** – Source IP address.
- **Source Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

WEB INTERFACE

To add rules to a Standard IP ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range.
9. Click Apply.

Figure 103: Configuring a Standard IPv4 ACL



CONFIGURING AN EXTENDED IPV4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Extended) page to configure an Extended IPv4 ACL.

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.

- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 178.)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Service Type** – Packet priority settings based on the following criteria:
  - **ToS** – Type of Service level. (Range: 0-15)
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **DSCP** – DSCP priority level. (Range: 0-63)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63)

  The control bit mask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

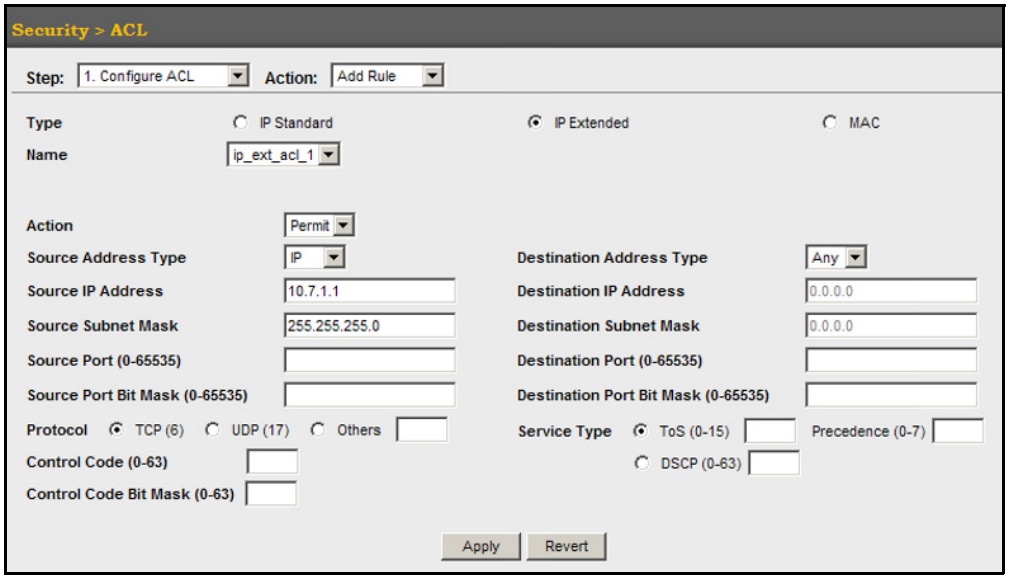
  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use control-code 2, control bit mask 2
  - Both SYN and ACK valid, use control-code 18, control bit mask 18
  - SYN valid and ACK invalid, use control-code 2, control bit mask 18

WEB INTERFACE

To add rules to an Extended IP ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Extended from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range.
9. Set any other required criteria, such as service type, protocol type, or control code.
10. Click Apply.

Figure 104: Configuring an Extended IPv4 ACL



CONFIGURING A MAC ACL

Use the Security > ACL (Configure ACL - Add Rule - MAC) page to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **Tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.
- **VID** – VLAN ID. (Range: 1-4094)
- **VID Bit Mask** – VLAN bit mask. (Range: 1-4094)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex.)

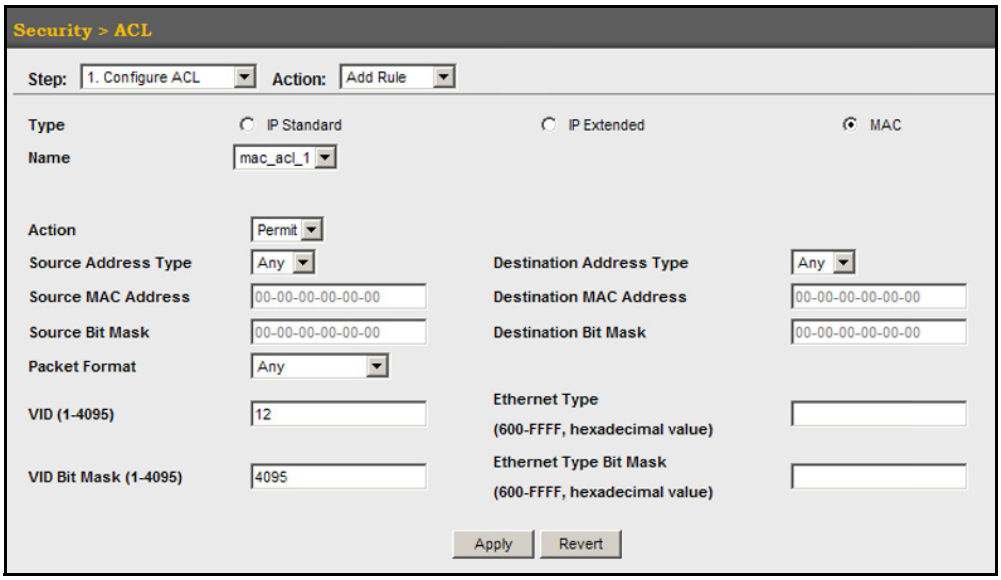
  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 600-ffff hex.)

WEB INTERFACE

To add rules to a MAC ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select MAC from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or MAC).
8. If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexadecimal bit mask for an address range.
9. Set any other required criteria, such as VID, Ethernet type, or packet format.
10. Click Apply.

Figure 105: Configuring a MAC ACL



BINDING A PORT TO AN ACCESS CONTROL LIST

After configuring ACLs, use the Security > ACL (Configure Interface) page to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

COMMAND USAGE

- This switch supports ACLs for ingress filtering only.
- You only bind one ACL to any port for ingress filtering.

PARAMETERS

These parameters are displayed:

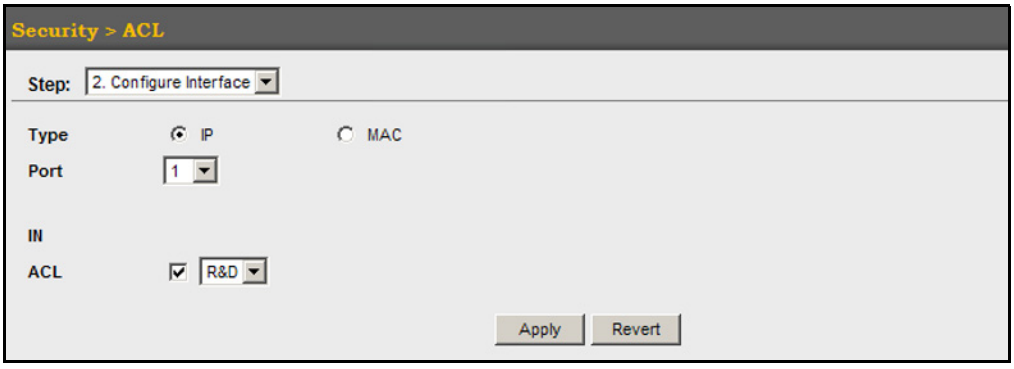
- **Type** – Selects the type of ACLs to bind to a port.
- **Port** – Fixed port or SFP module. (ES-2026/P: 1-26, ES-2024G/P: 1-24)
- **ACL** – ACL used for ingress packets.

WEB INTERFACE

To bind an ACL to a port:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select IP or MAC from the Type list.
4. Select a port.
5. Select the name of an ACL from the ACL list.
6. Click Apply.

Figure 106: Binding a Port to an ACL



FILTERING IP ADDRESSES FOR MANAGEMENT ACCESS

Use the Security > IP Filter page to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface or SNMP.

COMMAND USAGE

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP or web access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP or web), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

PARAMETERS

These parameters are displayed:

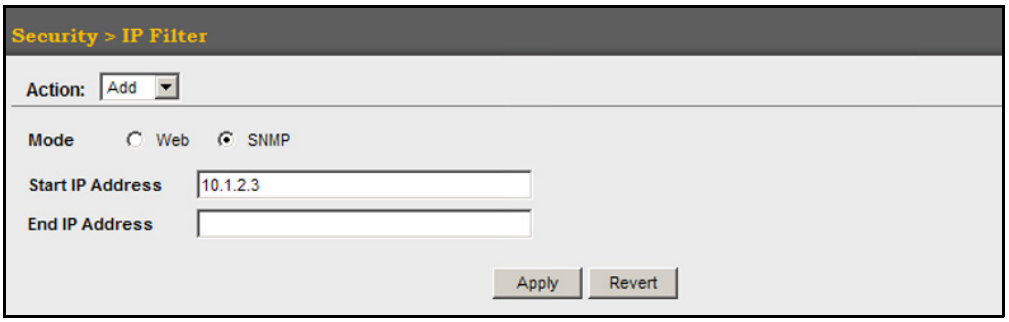
- **Mode**
  - **Web** – Configures IP address(es) for the web group.
  - **SNMP** – Configures IP address(es) for the SNMP group.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

WEB INTERFACE

To create a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Add from the Action list.
3. Select the management interface to filter (Web, SNMP).
4. Enter the IP addresses or range of addresses that are allowed management access to an interface.
5. Click Apply

Figure 107: Creating an IP Address Filter for Management Access



To show a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Show from the Action list.

Figure 108: Showing IP Addresses Authorized for Management Access



CONFIGURING PORT SECURITY

Use the Security > Port Security page to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

COMMAND USAGE

- The default maximum number of MAC addresses allowed on a secure port is zero (that is, disabled). To use port security, you must configure the maximum number of addresses allowed on a port.

- To configure the maximum number of address entries which can be learned on a port, first disable port security on a port, and then specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.

  Note that you can manually add additional secure addresses to a port using the Static Address Table (page 101).

- If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.

- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Interface > Port > General page (page 65).

- A secure port has the following restrictions:
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.

PARAMETERS

These parameters are displayed:

- **Port** – Port number.

- **Action** – Indicates the action to be taken when a port security violation is detected:

- **None**: No action should be taken. (This is the default.)
- **Trap**: Send an SNMP trap message.
- **Shutdown**: Disable the port.
- **Trap and Shutdown**: Send an SNMP trap message and disable the port.

- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

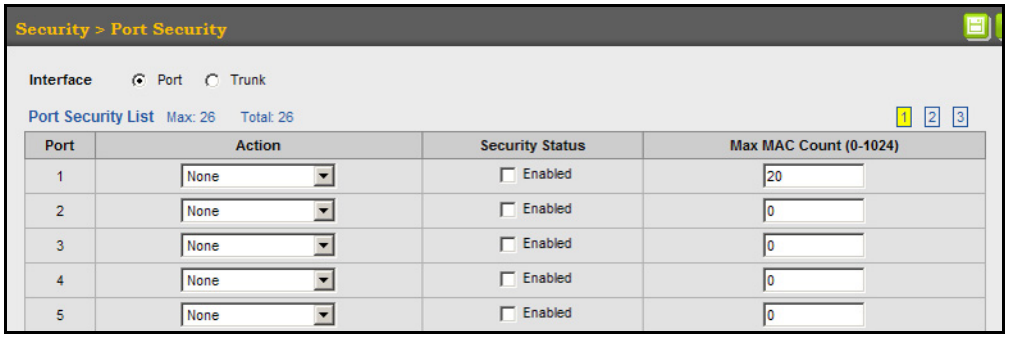
  The maximum address count is effective when port security is enabled or disabled, but can only be set when Security Status is disabled.

WEB INTERFACE

To set the maximum number of addresses which can be learned on a port:

1. Click Security, Port Security.
2. If port security is enabled on the selected port, first clear the check box in Security Status column to disable security.
3. Set the maximum number of MAC addresses allowed on the port.
4. Click Apply.

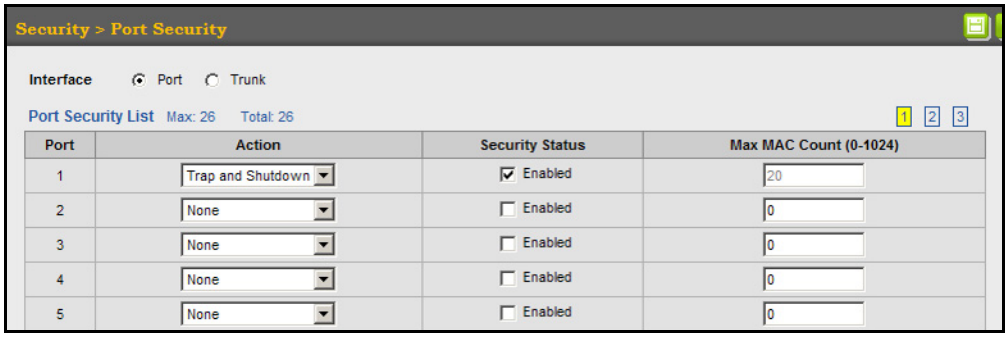
Figure 109: Setting the Maximum Address Count for Port Security



To enable port security:

1. Click Security, Port Security.
2. Set the action to take when an invalid address is detected on a port.
3. Mark the check box in the Security Status column to enable security.
4. Click Apply.

Figure 110: Configuring the Status and Response for Port Security



CONFIGURING 802.1X PORT AUTHENTICATION

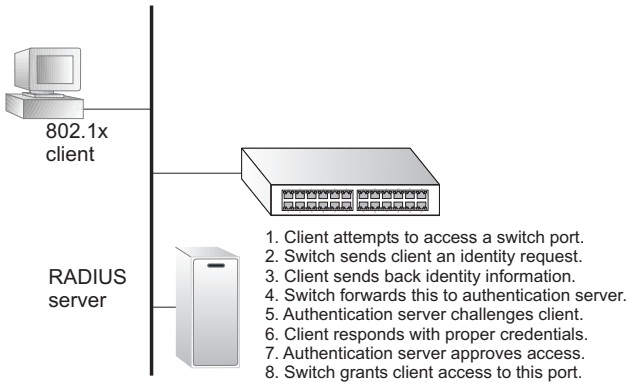
Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). The

client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked. In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Figure 111: Configuring Port Security


802.1x
client
RADIUS
server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

The operation of 802.1X on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1X "Auto" mode.
- Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5, PEAP, TLS, or TTLS. (Native support for these encryption methods is provided in Windows XP, and in Windows 2000 with Service Pack 4. To support these encryption methods in Windows 95 and 98, you can use the AEGIS dot1x client or other comparable client software)

CONFIGURING 802.1X GLOBAL SETTINGS

Use the Security > Port Authentication (Configure Global) page to configure IEEE 802.1X port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

PARAMETERS

These parameters are displayed:

- **Port Authentication Status** – Sets the global setting for 802.1X. (Default: Disabled)
- **Identity Profile User Name** – The dot1x supplicant user name. (Range: 1-8 characters)

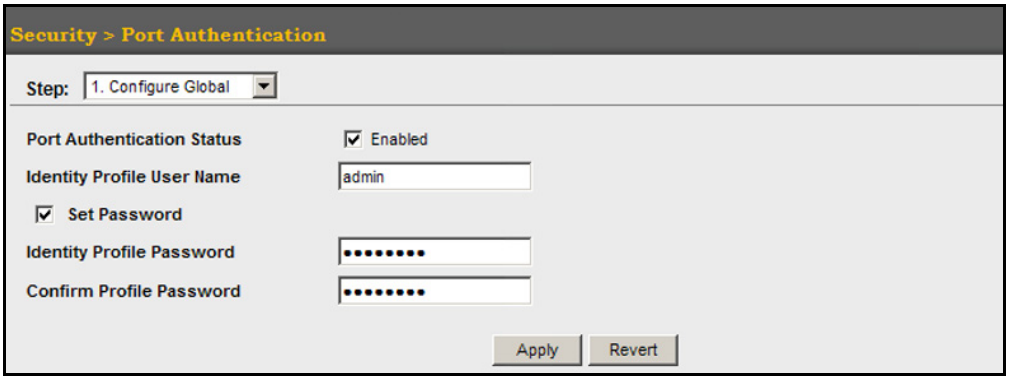
  The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see "Configuring Port Supplicant Settings for 802.1X" on page 196).
- **Set Password** – Allows the dot1x supplicant password to be entered.
- **Identity Profile Password** – The dot1x supplicant password used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. (Range: 1-8 characters)
- **Confirm Profile Password** – This field is used to confirm the dot1x supplicant password.

WEB INTERFACE

To configure global settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Global from the Step list.
3. Enable 802.1X globally for the switch. Then set the user name and password to use when the switch responds an MD5 challenge from the authentication server.
4. Click Apply

Figure 112: Configuring Global Settings for 802.1X Port Authentication



CONFIGURING PORT AUTHENTICATOR SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface – Authenticator) page to configure 802.1X port settings for the switch as the local authenticator. When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

COMMAND USAGE

- When the switch functions as a local authenticator between supplicant devices attached to the switch and the authentication server, configure the parameters for the exchange of EAP messages between the authenticator and clients on the Authenticator configuration page.
- When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters on the Configure Global page (see "Configuring 802.1X Global Settings" on page 191) which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator (see "Configuring Port Supplicant Settings for 802.1X" on page 196).
- This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on this configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on this page and enabling the PAE supplicant on the Supplicant configuration page.

PARAMETERS

These parameters are displayed:

- **Port** – Port number.
- **Status** – Indicates if authentication is enabled or disabled on the port. The status is disabled if the control mode is set to Force-Authorized.

- **Authorized** – Displays the 802.1X authorization status of connected clients.
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Control Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Default: Single-Host)
  - **Single-Host** – Allows only a single host to connect to this port.
  - **Multi-Host** – Allows multiple host to connect to this port.

    In this mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- **Max MAC Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- **Max-Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Quiet Period** – Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Tx Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Supplicant Timeout** – Sets the time that a switch port waits for a response to an EAP request from a client before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

This command attribute sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

- **Server Timeout** – Sets the time that a switch port waits for a response to an EAP request from an authentication server before re-transmitting an EAP packet. (Fixed Setting: 10 seconds)

- **Re-authentication Status** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)

- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

Authenticator PAE State Machine

- **State** – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).

- **Reauth Count** – Number of times connecting state is re-entered.

- **Current Identifier** – Identifier sent in each EAP Success, Failure or Request packet by the Authentication Server.

Backend State Machine

- **State** – Current state (including request, response, success, fail, timeout, idle, initialize).

- **Request Count** – Number of EAP Request packets sent to the Supplicant without receiving a response.

- **Identifier (Server)** – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

Reauthentication State Machine

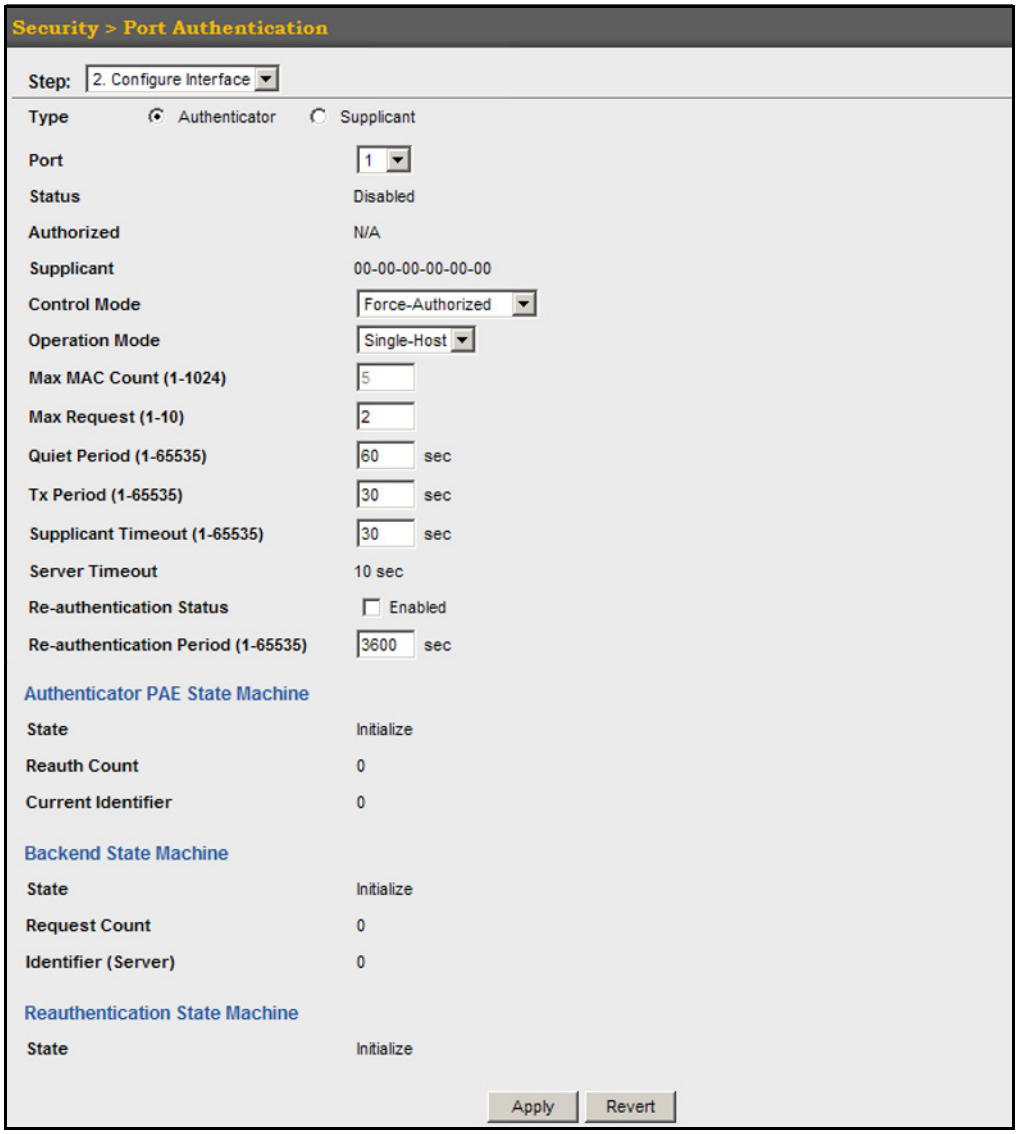
- **State** – Current state (including initialize, reauthenticate).

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Click Authenticator.
4. Modify the authentication settings for each port as required.
5. Click Apply

Figure 113: Configuring Interface Settings for 802.1X Port Authenticator



CONFIGURING PORT SUPPLICANT SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface – Supplicant) page to configure 802.1X port settings for supplicant requests issued from a port to an authenticator on another device. When 802.1X is enabled and the control mode is set to Force-Authorized (see "Configuring Port Authenticator Settings for 802.1X" on page 192), you need to configure the parameters for the client supplicant process if the client must be authenticated through another device in the network.

COMMAND USAGE

- When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters on the Configure Global page (see "Configuring 802.1X Global Settings" on page 191) which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator on this configuration page. When PAE supplicant mode is enabled on a port, it will not respond to dot1x messages meant for an authenticator.

- This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on the Authenticator configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on that configuration page and enabling the PAE supplicant on the Supplicant configuration page.

PARAMETERS

These parameters are displayed:

- **Port** – Port number.

- **PAE Supplicant** – Enables PAE supplicant mode. (Default: Disabled)

  If the attached client must be authenticated through another device in the network, supplicant status must be enabled.

  Supplicant status can only be enabled if PAE Control Mode is set to "Force-Authorized" on this port (see "Configuring Port Authenticator Settings for 802.1X" on page 192).

  PAE supplicant status cannot be enabled if a port is a member of trunk or LACP is enabled on the port.

- **Authentication Period** – The time that a supplicant port waits for a response from the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)

- **Hold Period** – The time that a supplicant port waits before resending its credentials to find a new an authenticator. (Range: 1-65535 seconds; Default: 30 seconds)

- **Start Period** – The time that a supplicant port waits before resending an EAPOL start frame to the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)

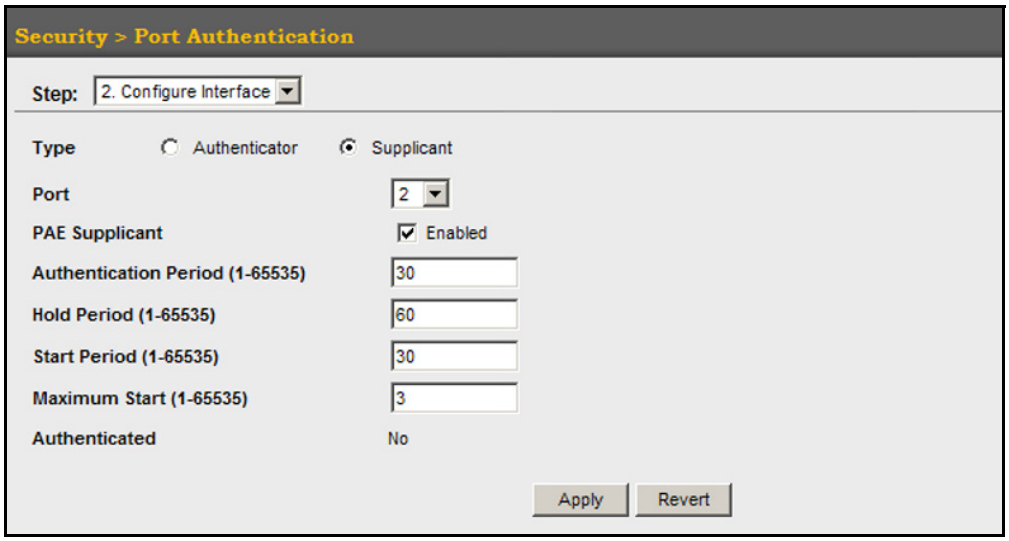
- **Maximum Start** – The maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. (Range: 1-65535; Default: 3)
- **Authenticated** – Shows whether or not the supplicant has been authenticated.

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Click Supplicant.
4. Modify the supplicant settings for each port as required.
5. Click Apply

Figure 114: Configuring Interface Settings for 802.1X Port Supplicant



DISPLAYING 802.1X STATISTICS

Use the Security > Port Authentication (Show Statistics) page to display statistics for dot1x protocol exchanges for any port.

PARAMETERS

These parameters are displayed:

Table 18: 802.1X Statistics

Parameter	Description
Authenticator	
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Authenticator.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Supplicant	
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Supplicant in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Supplicant.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Supplicant.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Supplicant.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Supplicant.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Supplicant.
Rx EAP LenError	The number of EAPOL frames that have been received by this Supplicant in which the Packet Body Length field is invalid.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Supplicant.

Table 18: 802.1X Statistics (Continued)

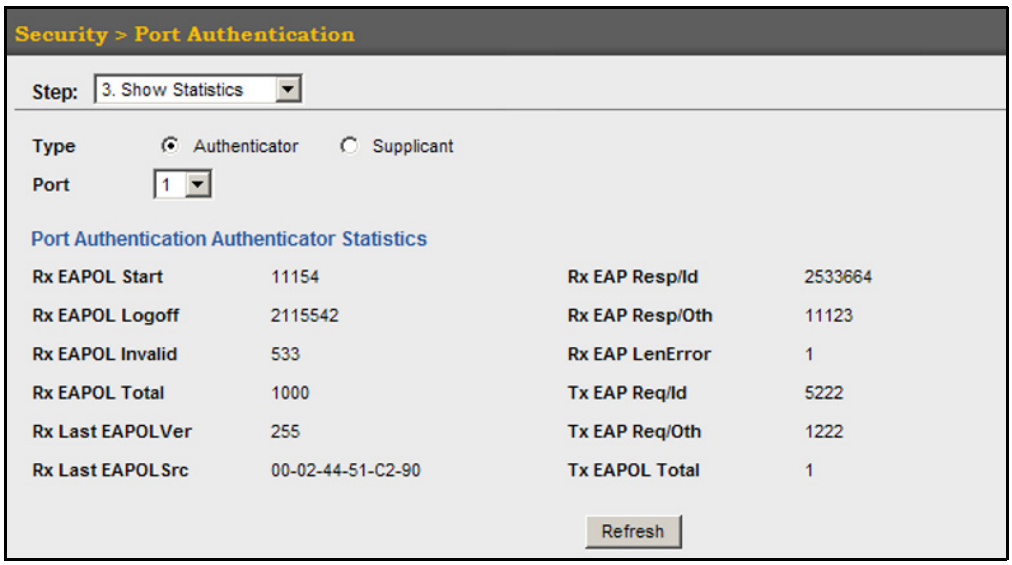
Parameter	Description
Tx EAPOL Start	The number of EAPOL Start frames that have been transmitted by this Supplicant.
Tx EAPOL Logoff	The number of EAPOL Logoff frames that have been transmitted by this Supplicant.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Supplicant.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Supplicant.

WEB INTERFACE

To display port authenticator statistics for 802.1X:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Click Authenticator.

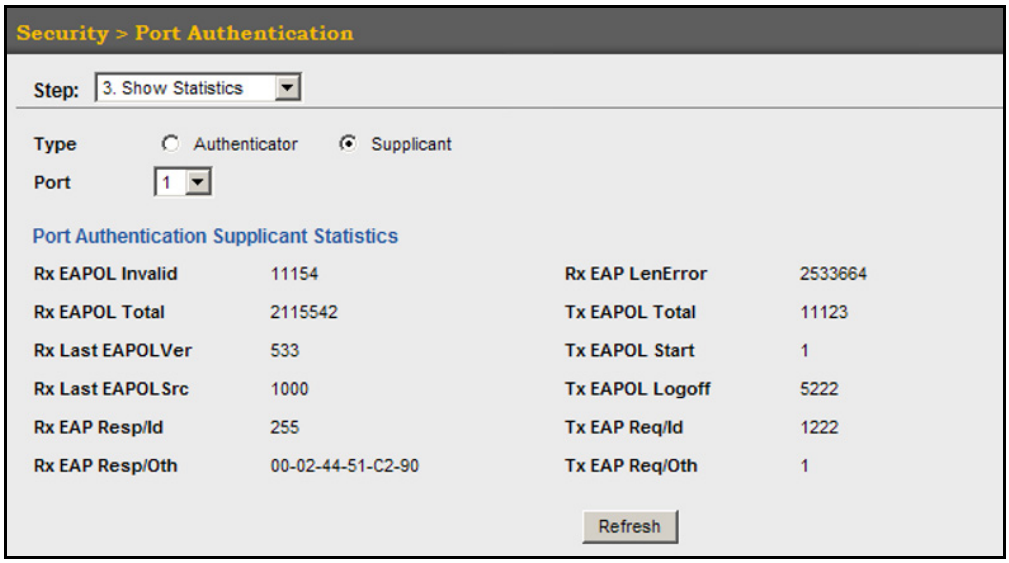
Figure 115: Showing Statistics for 802.1X Port Authenticator



To display port supplicant statistics for 802.1X:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Click Supplicant.

Figure 116: Showing Statistics for 802.1X Port Supplicant



15 BASIC ADMINISTRATION PROTOCOLS

This chapter describes basic administration tasks including:

- Event Logging – Sets conditions for logging event messages to system memory or flash memory, configures conditions for sending trap messages to remote log servers, and configures trap reporting to remote hosts using Simple Mail Transfer Protocol (SMTP).
- Link Layer Discovery Protocol (LLDP) – Configures advertisement of basic information about the local switch, or discovery of information about neighboring devices on the local broadcast domain.
- Power over Ethernet – Sets the priority and power budget for each port.
- Simple Network Management Protocol (SNMP) – Configures switch management through SNMPv1, SNMPv2c or SNMPv3.
- Remote Monitoring (RMON) – Configures local collection of detailed statistics or events which can be subsequently retrieved through SNMP.
- Switch Clustering – Configures centralized management by a single unit over a group of switches connected to the same local network

CONFIGURING EVENT LOGGING

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

SYSTEM LOG CONFIGURATION

Use the Administration > Log > System (Configure Global) page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

PARAMETERS

These parameters are displayed:

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 19: Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

NOTE: The Flash Level must be equal to or less than the RAM Level.

NOTE: All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).

NOTE: All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

WEB INTERFACE

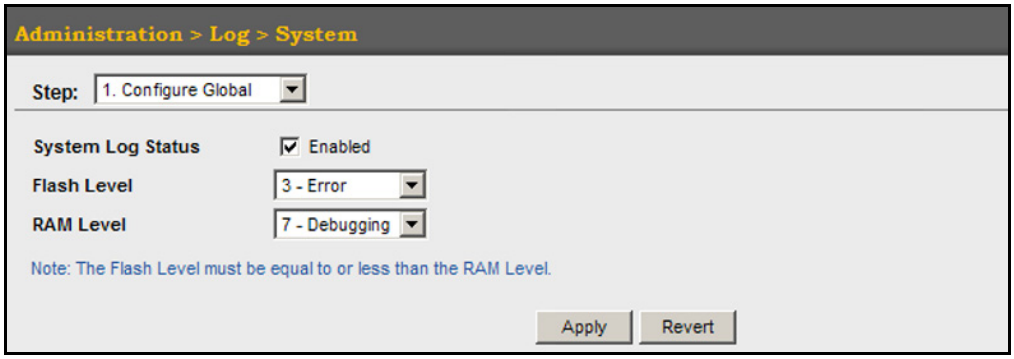
To configure the logging of error messages to system memory:

1. Click Administration, Log, System.
2. Select Configure Global from the Step list.

3. Enable or disable system logging, set the level of event messages to be logged to flash memory and RAM.

4. Click Apply.

Figure 117: Configuring Settings for System Memory Logs



To show the error messages logged to system or flash memory:

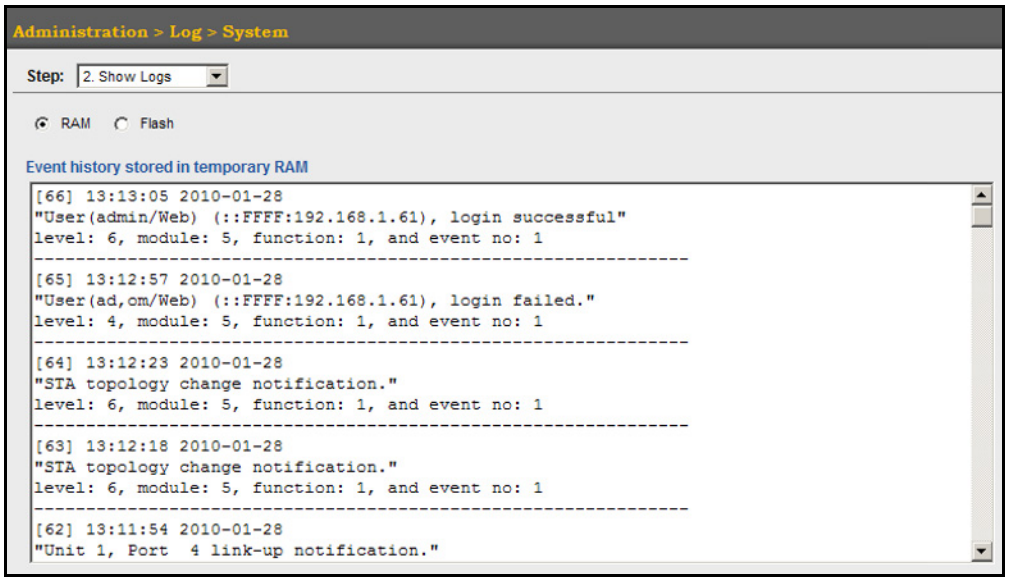
1. Click Administration, Log, System.

2. Select Show Logs from the Step list.

3. Click RAM to display log messages stored in system memory, or Flash to display messages stored in flash memory.

   This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Figure 118: Showing Error Messages Logged to System Memory


Administration > Log > System
Step: 2. Show Logs
RAM
Flash
Event history stored in temporary RAM
[66] 13:13:05 2010-01-28
"User(admin/Web) (::FFFF:192.168.1.61), login successful"
level: 6, module: 5, function: 1, and event no: 1
[65] 13:12:57 2010-01-28
"User(ad,om/Web) (::FFFF:192.168.1.61), login failed."
level: 4, module: 5, function: 1, and event no: 1
[64] 13:12:23 2010-01-28
"STA topology change notification."
level: 6, module: 5, function: 1, and event no: 1
[63] 13:12:18 2010-01-28
"STA topology change notification."
level: 6, module: 5, function: 1, and event no: 1
[62] 13:11:54 2010-01-28
"Unit 1, Port 4 link-up notification."

REMOTE LOG CONFIGURATION

Use the Administration > Log > Remote page to send log messages to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

PARAMETERS

These parameters are displayed:

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

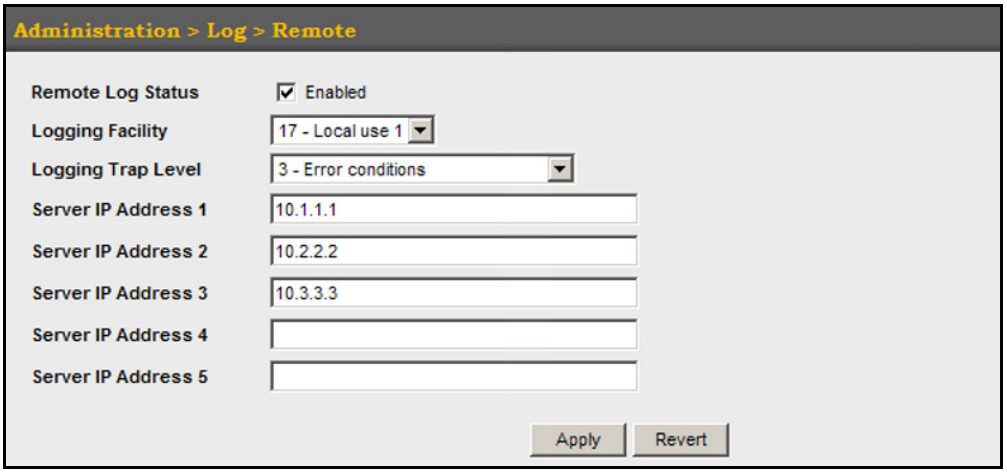
  The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Server IP Address** – Specifies the IP address of a remote server which will be sent syslog messages.

WEB INTERFACE

To configure the logging of error messages to remote servers:

1. Click Administration, Log, Remote.
2. Enable remote logging, specify the facility type to use for the syslog messages. and enter the IP address of the remote servers.
3. Click Apply.

Figure 119: Configuring Settings for Remote Logging of Error Messages



LINK LAYER DISCOVERY PROTOCOL

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

SETTING LLDP TIMING ATTRIBUTES

Use the Administration > LLDP (Configure Global) page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

PARAMETERS

These parameters are displayed:

- **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)
- **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

  This attribute must comply with the following rule:
  (Transmission Interval * Hold Time Multiplier) ≤ 65536, and
  Transmission Interval >= (4 * Delay Interval)
- **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:
  (Transmission Interval * Holdtime Multiplier) ≤ 65536.

  Therefore, the default TTL is 4*30 = 120 seconds.
- **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

  The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

  This attribute must comply with the rule:
  (4 * Delay Interval) ≤ Transmission Interval
- **Reinitialization Delay** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

  When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.
- **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

  This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

  Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the

time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets)

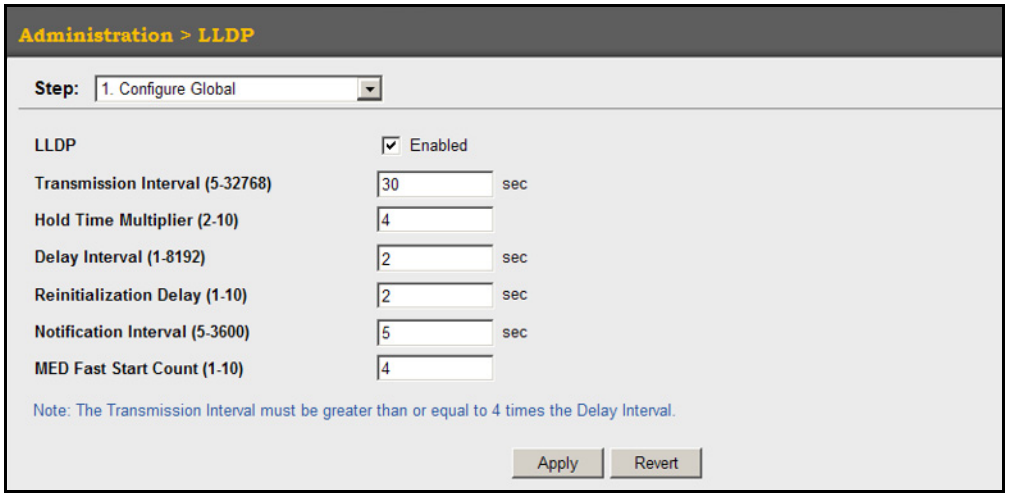
  The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

WEB INTERFACE

To configure LLDP timing attributes:

1. Click Administration, LLDP.
2. Select Configure Global from the Step list.
3. Enable LLDP, and modify any of the timing parameters as required.
4. Click Apply.

Figure 120: Configuring LLDP Timing Attributes



CONFIGURING LLDP INTERFACE ATTRIBUTES

Use the Administration > LLDP (Configure Interface – Configure General) page to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

PARAMETERS

These parameters are displayed:

- **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)
- **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Disabled)

  This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

  For information on defining SNMP trap destinations, see "Specifying Trap Managers" on page 245.

  Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.
- **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Enabled)
- **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.
  - **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

    The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

    Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

- **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

- **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

- **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

- **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see "Displaying System Information" on page 47.

◆ **802.1 Organizationally Specific TLVs** – Configures IEEE 802.1 information included in the TLV field of advertised messages.

- **Protocol Identity** – The protocols that are accessible through this interface.

- **VLAN ID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see "IEEE 802.1Q VLANs" on page 93).

- **VLAN Name** – The name of all VLANs to which this interface has been assigned (see "IEEE 802.1Q VLANs" on page 93).

- **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface (see "IEEE 802.1Q VLANs" on page 93).

◆ **802.3 Organizationally Specific TLVs** – Configures IEEE 802.3 information included in the TLV field of advertised messages.

- **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.

- **Max Frame Size** – The maximum frame size. (See "Configuring Support for Jumbo Frames" on page 50 for information on configuring the maximum frame size for this switch

- **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

- **PoE** – Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

◆ **MED TLVs** – Configures general information included in the MED TLV field of advertised messages.

- **Capabilities** – This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

- **Extended Power** – This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode). Note that this device does not support PoE capabilities.

- **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

- **Location** – This option advertises location identification details.

- **Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

◆ **MED-Location Civic Address** – Configures information for the location of the attached device included in the MED TLV field of advertised messages, including the country and the device type.

- **Country** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

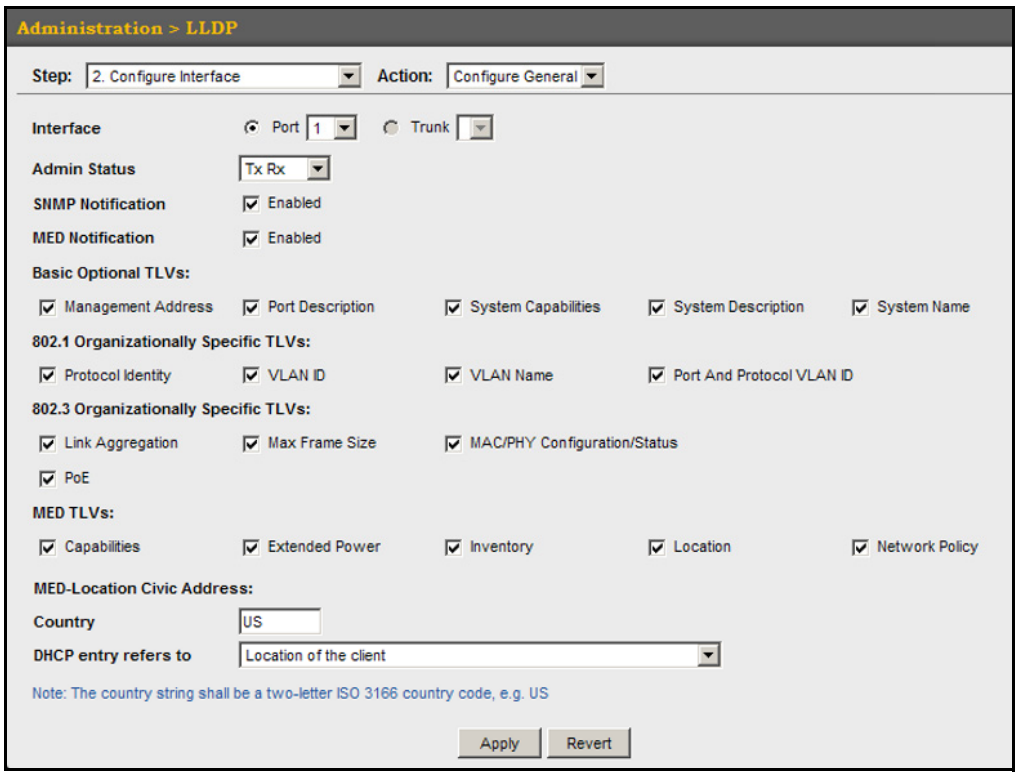
- **Device entry refers to** – The type of device to which the location applies:
  - Location of DHCP server.
  - Location of network element closest to client.
  - Location of client. (This is the default.)

WEB INTERFACE

To configure LLDP interface attributes:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Configure General from the Action list.
4. Select an interface from the Port or Trunk list.
5. Set the LLDP transmit/receive mode, specify whether or not to send SNMP trap messages, and select the information to advertise in LLDP messages.
6. Click Apply.

Figure 121: Configuring LLDP Interface Attributes



CONFIGURING LLDP INTERFACE CIVIC-ADDRESS

Use the Administration > LLDP (Configure Interface – Add CA-Type) page to specify the physical location of the device attached to an interface.

COMMAND USAGE

- Use the Civic Address type (CA-Type) to advertise the physical location of the device attached to an interface, including items such as the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address type defined in

RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 20: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

- Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

PARAMETERS

These parameters are displayed:

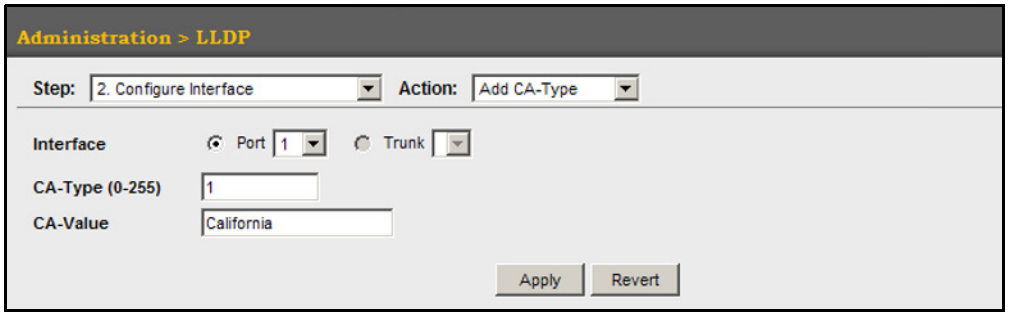
- **CA-Type** – Descriptor of the data civic address value. (Range: 0-255)
- **CA-Value** – Description of a location. (Range: 1-32 characters)

WEB INTERFACE

To specify the physical location of the attached device:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Add CA-Type from the Action list.
4. Select an interface from the Port or Trunk list.
5. Specify a CA-Type and CA-Value pair.
6. Click Apply.

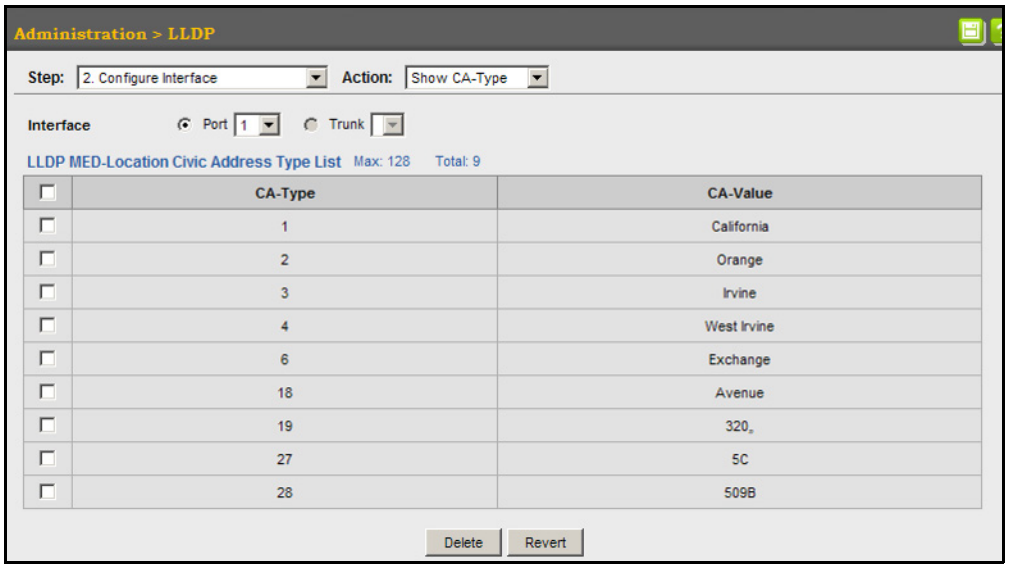
Figure 122: Configuring the Civic Address for an LLDP Interface



To show the physical location of the attached device:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Show CA-Type from the Action list.
4. Select an interface from the Port or Trunk list.

Figure 123: Showing the Civic Address for an LLDP Interface



DISPLAYING LLDP LOCAL DEVICE INFORMATION

Use the Administration > LLDP (Show Local Device Information) page to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

PARAMETERS

These parameters are displayed:

Global Settings

- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

Table 21: Chassis ID Subtype

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system's administratively assigned name (see "Displaying System Information" on page 47).
- **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

Table 22: System Capabilities

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011

Table 22: System Capabilities (Continued)

ID Basis	Reference
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.
- **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

WEB INTERFACE

To display LLDP information for the local device:

1. Click Administration, LLDP.
2. Select Show Local Device Information from the Step list.
3. Select General, Port, or Trunk.

Figure 124: Displaying Local Device Information for LLDP (General)

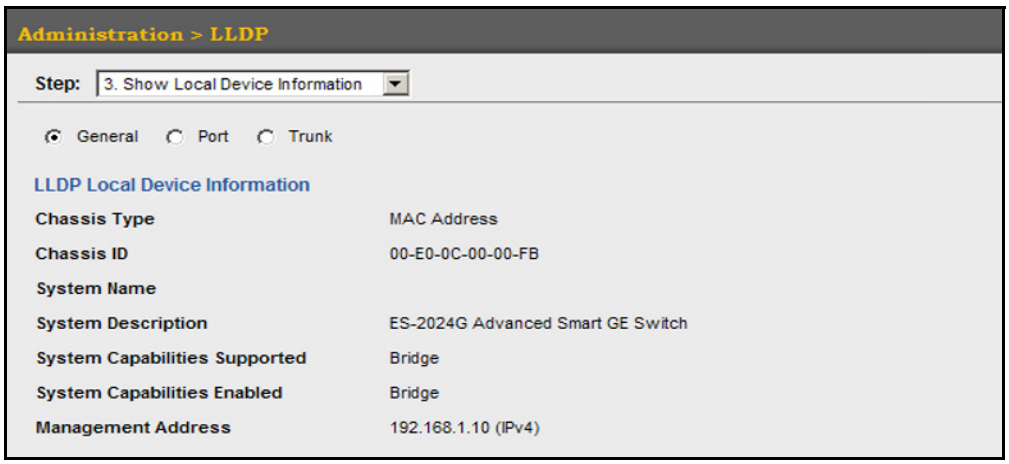
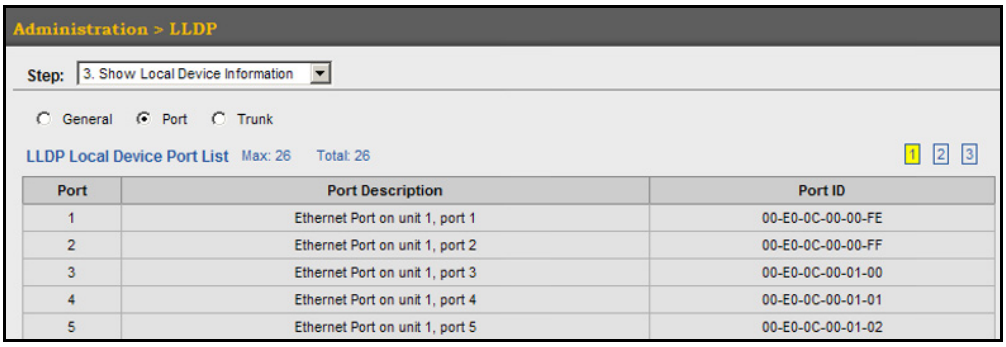


Figure 125: Displaying Local Device Information for LLDP (Port)



DISPLAYING LLDP REMOTE PORT INFORMATION

Use the Administration > LLDP (Show Remote Device Information) page to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

PARAMETERS

These parameters are displayed:

Port

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Name** – A string that indicates the system's administratively assigned name.

Port Details

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. (See Table 21, "Chassis ID Subtype," on page 214.)
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system's assigned name.

- **System Description** – A textual description of the network entity.
- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

Table 23: Port ID Subtype

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

- **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system. (See Table 22, "System Capabilities," on page 214.)
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See Table 22, "System Capabilities," on page 214.)
- **Management Address List** – The management addresses for this device. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

  If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Port Details – 802.1 Extension Information

- **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
- **Remote Port-Protocol VLAN List** – The port-based protocol VLANs configured on this interface, whether the given port (associated with the remote system) supports port-based protocol VLANs, and whether the port-based protocol VLANs are enabled on the given port associated with the remote system.

- **Remote VLAN Name List** – VLAN names associated with a port.
- **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity, and an octet string used to identify the protocols associated with a port of the remote system.

Port Details – 802.3 Extension Port Information

- **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.
- **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

Table 24: Remote Port Auto-Negotiation Advertised Capability

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

- **Remote Port Auto-Neg Status** – Shows whether port auto-negotiation is enabled on a port associated with the remote system.
- **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID.

Port Details – 802.3 Extension Power Information

- **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).
- **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.
- **Remote Power Pairs** – "Signal" means that the signal pairs only are in use, and "Spare" means that the spare pairs only are in use.
- **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.
- **Remote Power Pair Controlable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.
- **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements.

Port Details – 802.3 Extension Trunk Information

- **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.
- **Remote Link Aggregation Status** – The current aggregation status of the link.
- **Remote Link Aggregation Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero.

Port Details – 802.3 Extension Frame Information

- **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

WEB INTERFACE

To display LLDP information for a remote port:

1. Click Administration, LLDP.
2. Select Show Remote Device Information from the Step list.
3. Select Port, Port Details, Trunk, or Trunk Details.

Figure 126: Displaying Remote Device Information for LLDP (Port)

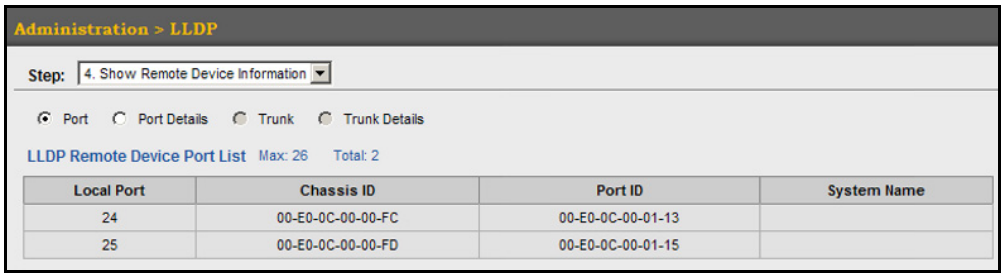
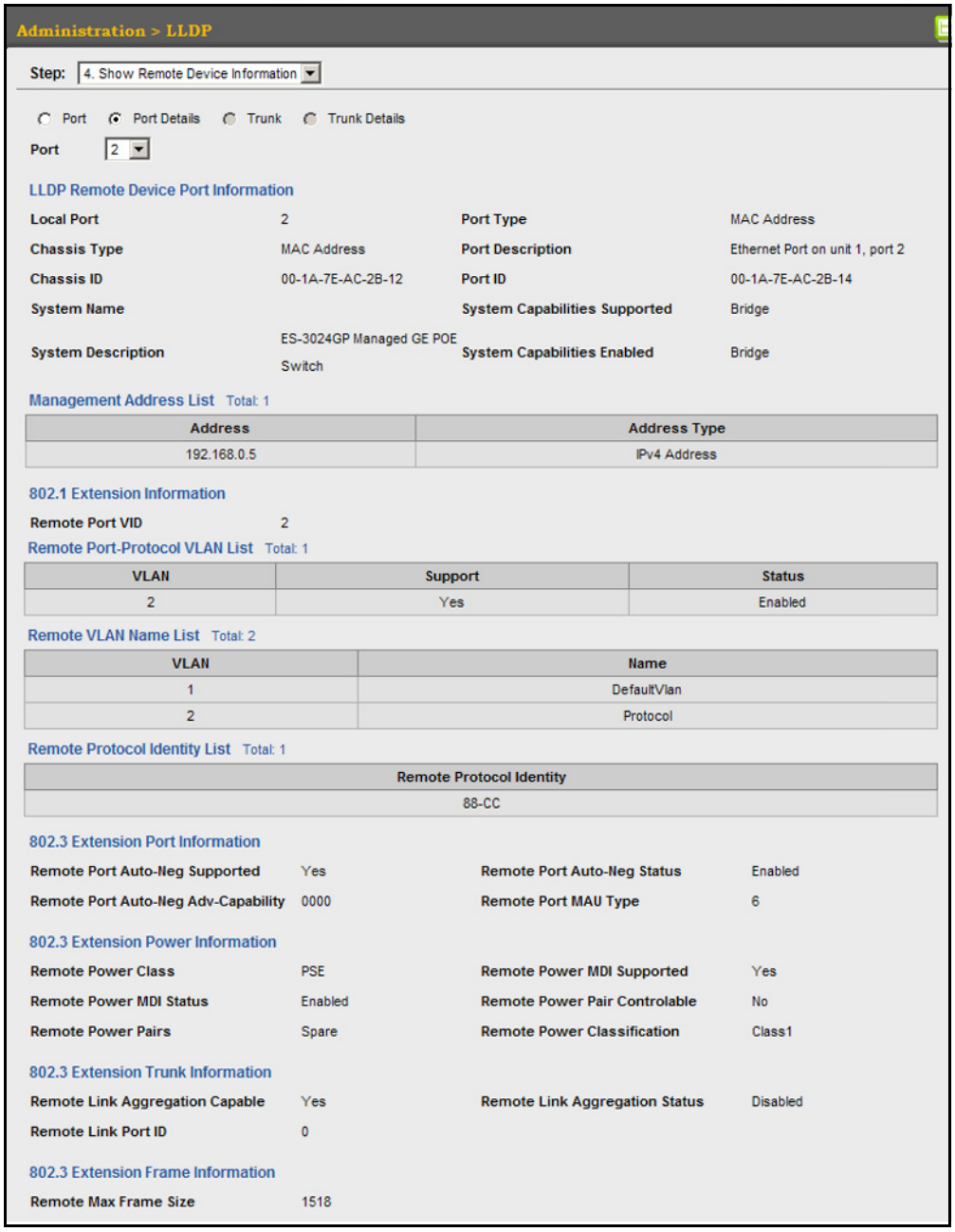


Figure 127: Displaying Remote Device Information for LLDP (Port Details)



DISPLAYING DEVICE STATISTICS

Use the Administration > LLDP (Show Device Statistics) page to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

PARAMETERS

These parameters are displayed:

General Statistics on Remote Devices

- **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.

- **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
- **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Port/Trunk

- **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
- **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.
- **Frames Received** – Number of LLDP PDUs received.
- **Frames Sent** – Number of LLDP PDUs transmitted.
- **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

WEB INTERFACE

To display statistics for LLDP-capable devices attached to the switch:

1. Click Administration, LLDP.
2. Select Show Device Statistics from the Step list.
3. Select General, Port, or Trunk.

Figure 128: Displaying LLDP Device Statistics (General)

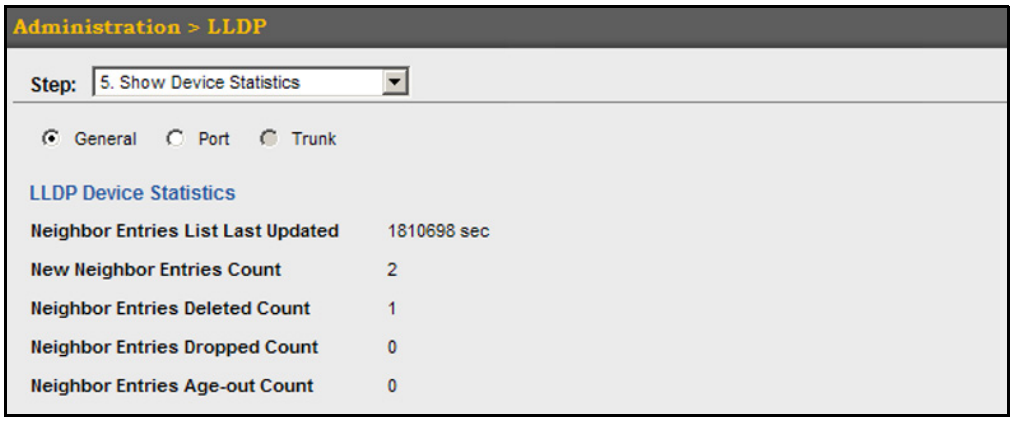
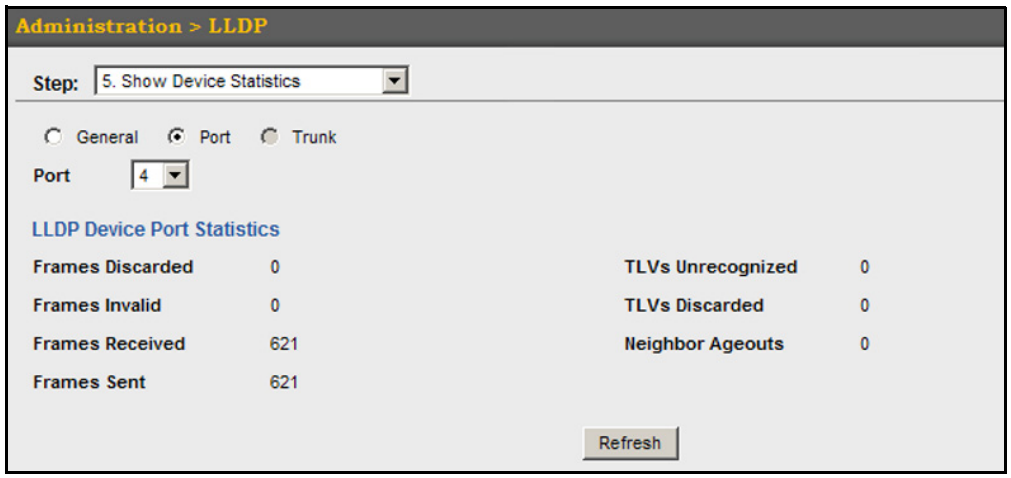

Administration > LLDP
Step: 5. Show Device Statistics
General Port Trunk
LLDP Device Statistics
Neighbor Entries List Last Updated 1810698 sec
New Neighbor Entries Count 2
Neighbor Entries Deleted Count 1
Neighbor Entries Dropped Count 0
Neighbor Entries Age-out Count 0

Figure 129: Displaying LLDP Device Statistics (Port)



POWER OVER ETHERNET

The switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-compliant devices (IEEE 802.3af or 802.3at).

The switch's power management enables individual port power to be controlled within the switch's power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Ports can be set to one of four power priority levels, critical, high, medium, or low. To control the power supply within the switch's budget, ports set at critical to medium priority have power enabled in preference to those ports set at low priority. For example, when a device connected to a port is set to critical priority, the switch supplies the required power, if necessary by denying power to ports set for a lower priority during bootup. If a device is connected to a switch port and the switch detects that it requires more than the power budget of the port, no power is supplied to the device (i.e., port power remains off).

If the power demand from devices connected to switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:

- If a device is connected to a low-priority port and causes the switch to exceed its budget, port power is not turned on.
- If a device is connected to a critical or high-priority port and would cause the switch to exceed its power budget as determined during booting up, power is provided to the port only if the switch can drop power to one or more lower-priority ports and thereby remain within its overall budget.
- If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port.

NOTE: Power is dropped from low-priority ports in sequence starting from port number 1.

NOTE: For more information on using the PoE provided by this switch refer to the Installation Guide.

DISPLAYING THE SWITCH'S OVERALL POE POWER BUDGET

Use the Administration > PoE (Configure Global) page to display the maximum PoE power budget for the switch (power available to all Fast Ethernet ports). The maximum power budget is fixed at the maximum available setting, which prevents overload conditions at the power source. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

PARAMETERS

These parameters are displayed:

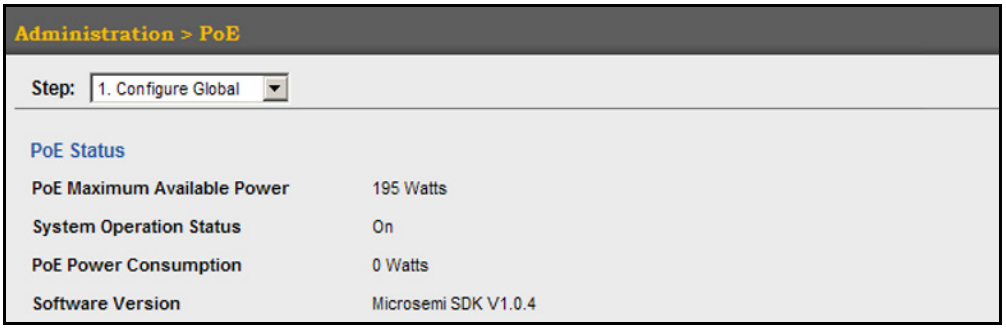
- **PoE Maximum Available Power** – The power budget for the switch. If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power. (Fixed: 195 Watts)
- **System Operation Status** – Status of the PoE power service provided to the switch ports.
- **PoE Power Consumption** – The amount of power being consumed by PoE devices connected to the switch.
- **Software Version** – The version of software running on the PoE controller subsystem in the switch.

WEB INTERFACE

To set the overall PoE power budget for switch:

1. Click Administration, PoE.
2. Select Configure Global from the Step list.

Figure 130: Showing the Switch's PoE Budget



SETTING THE PORT POE POWER BUDGET

Use the Administration > PoE (Configure Interface) page to set the maximum power provided to a port.

COMMAND USAGE

- The switch only provides power to the Fast Ethernet ports. It can supply up to 30W of power to the first six ports (based on the IEEE 802.3at draft), up to 15.4W to 12 ports (based on IEEE 802.3af). or up to 7.5 to 24 ports (based on IEEE 802.3af).
- If a device is connected to a switch port and the switch detects that it requires more than the power budget set for the port or to the overall switch, no power is supplied to the device (i.e., port power remains off).
- If the power demand from devices connected to all switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:
  - If a device is connected to a low-priority port and causes the switch to exceed its budget, power to this port is not turned on.
  - If a device is connected to a critical or high-priority port and causes the switch to exceed its budget, port power is turned on, but the switch drops power to one or more lower-priority ports.

NOTE: Power is dropped from low-priority ports in sequence starting from port number 1.

- If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port regardless of its priority setting.

PARAMETERS

These parameters are displayed:

- **Port** – The port number on the switch.
- **Admin Status** – Enables PoE power on a port. Power is automatically supplied when a device is detected on a port, providing that the power demanded does not exceed the switch or port power budget. (Default: Enabled)
- **Mode** – Shows whether or not PoE power is being supplied to a port.
- **Priority** – Sets the power priority for a port. (Options: Low, High, or Critical; Default: Low)
- **Power Allocation** – Sets the power budget for a port. (Range: 3000-30000 milliwatts on ports 1-6, 3000-15400 milliwatts on ports 7-24; Default: 30000 milliwatts on ports 1-6, 15400 milliwatts on ports 7-24)

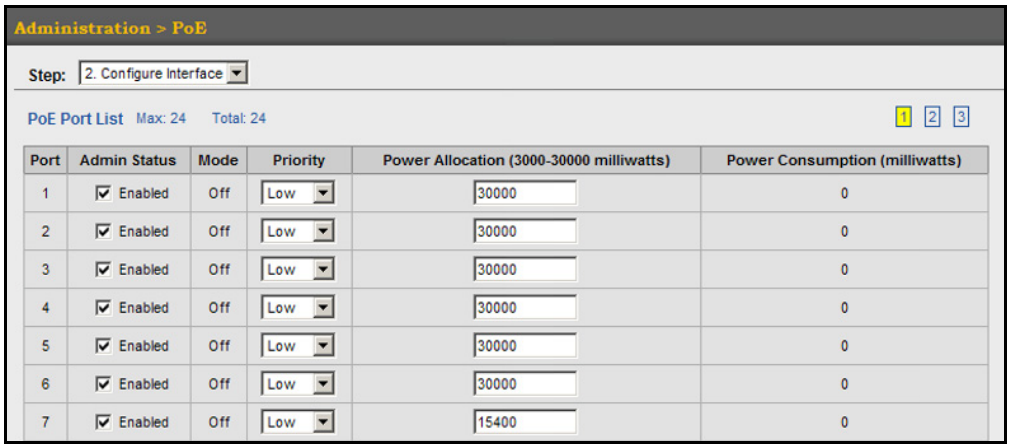
- **Power Consumption** – Current power consumption on a port.

WEB INTERFACE

To set the PoE power budget for a port:

1. Click Administration, PoE.
2. Select Configure Interface from the Step list.
3. Enable PoE power on selected ports. Set the priority and the power budget.
4. Click Apply.

Figure 131: Setting a Port's PoE Budget


Administration > PoE
Step: 2. Configure Interface
PoE Port List Max: 24 Total: 24
1 2 3
Port | Admin Status | Mode | Priority | Power Allocation (3000-30000 milliwatts) | Power Consumption (milliwatts)
1 | Enabled | Off | Low | 30000 | 0
2 | Enabled | Off | Low | 30000 | 0
3 | Enabled | Off | Low | 30000 | 0
4 | Enabled | Off | Low | 30000 | 0
5 | Enabled | Off | Low | 30000 | 0
6 | Enabled | Off | Low | 30000 | 0
7 | Enabled | Off | Low | 15400 | 0

SIMPLE NETWORK MANAGEMENT PROTOCOL

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using network management software.

Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 25: SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	A user name match only
v3	AuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

NOTE: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

COMMAND USAGE

Configuring SNMPv1/2c Management Access

To configure SNMPv1 or v2c management access to the switch, follow these steps:

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.

2. Use the Administration > SNMP (Configure User - Add Community) page to configure the community strings authorized for management access.

3. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

Configuring SNMPv3 Management Access

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.

2. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

3. Use the Administration > SNMP (Configure Engine) page to change the local engine ID. If you want to change the default engine ID, it must be changed before configuring other parameters.

4. Use the Administration > SNMP (Configure View) page to specify read and write access views for the switch MIB tree.

5. Use the Administration > SNMP (Configure User) page to configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).

6. Use the Administration > SNMP (Configure Group) page to assign SNMP users to groups, along with their specific authentication and privacy passwords.

CONFIGURING GLOBAL SETTINGS FOR SNMP

Use the Administration > SNMP (Configure Global) page to enable SNMPv3 service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.

PARAMETERS

These parameters are displayed:

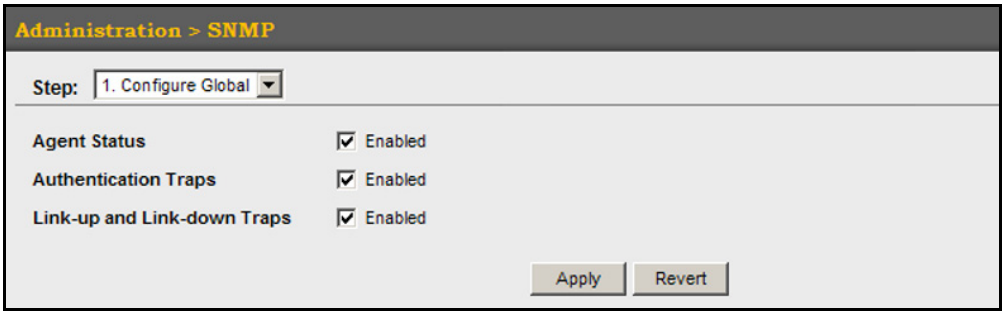
- **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- **Authentication Traps**[3] – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)
- **Link-up and Link-down Traps**[3] – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

WEB INTERFACE

To configure global settings for SNMP:

1. Click Administration, SNMP.
2. Select Configure Global from the Step list.
3. Enable SNMP and the required trap types.
4. Click Apply

Figure 132: Configuring Global Settings for SNMP



3. These are legacy notifications and therefore when used for SNMPv3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 233).

SETTING THE LOCAL ENGINE ID

Use the Administration > SNMP (Configure Engine - Set Engine ID) page to change the local engine ID. An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

COMMAND USAGE

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

PARAMETERS

These parameters are displayed:

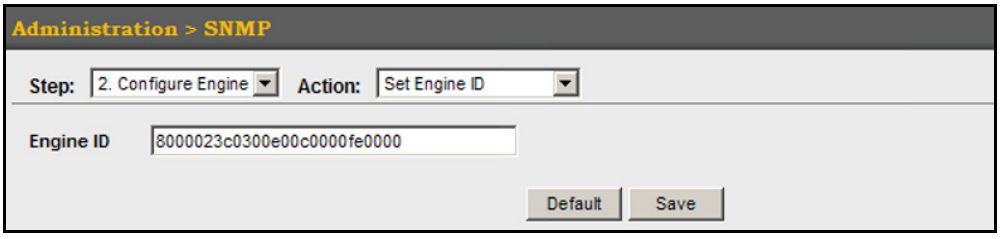
- **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".

WEB INTERFACE

To configure the local SNMP engine ID:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Set Engine ID from the Action list.
4. Enter an ID of a least 9 hexadecimal characters.
5. Click Apply

Figure 133: Configuring the Local Engine ID for SNMP



SPECIFYING A REMOTE ENGINE ID

Use the Administration > SNMP (Configure Engine - Add Remote Engine) page to configure a engine ID for a remote management station. To allow management access from an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host.

COMMAND USAGE

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Configuring Remote SNMPv3 Users" on page 243.)

PARAMETERS

These parameters are displayed:

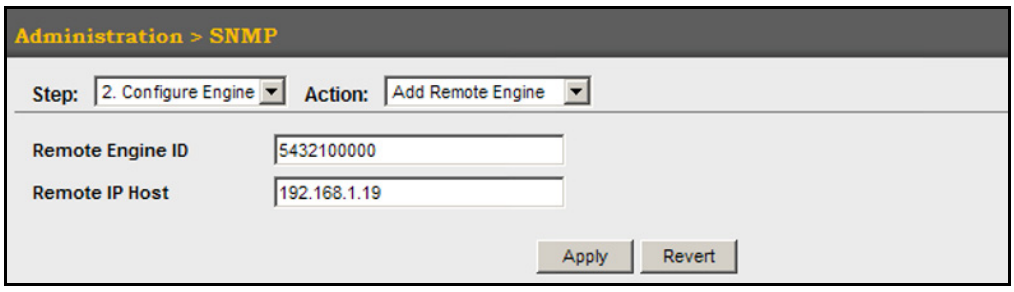
- **Remote Engine ID** – The engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".
- **Remote IP Host** – The IP address of a remote management station which is using the specified engine ID.

WEB INTERFACE

To configure a remote SNMP engine ID:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Add Remote Engine from the Action list.
4. Enter an ID of a least 9 hexadecimal characters, and the IP address of the remote host.
5. Click Apply

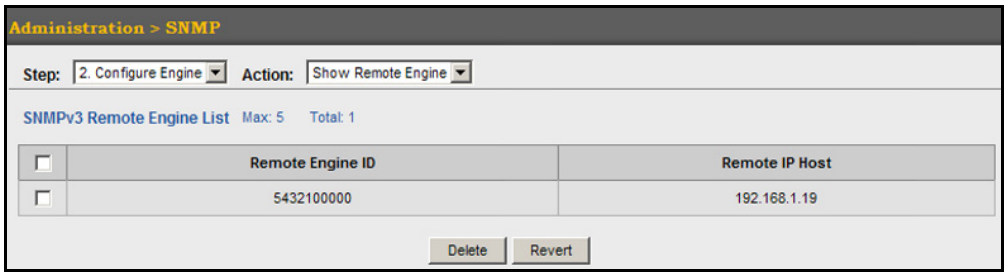
Figure 134: Configuring a Remote Engine ID for SNMP



To show the remote SNMP engine IDs:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Show Remote Engine from the Action list.

Figure 135: Showing Remote Engine IDs for SNMP



SETTING SNMPV3 VIEWS

Use the Administration > SNMP (Configure View) page to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

PARAMETERS

These parameters are displayed:

Add View

- **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Add OID Subtree

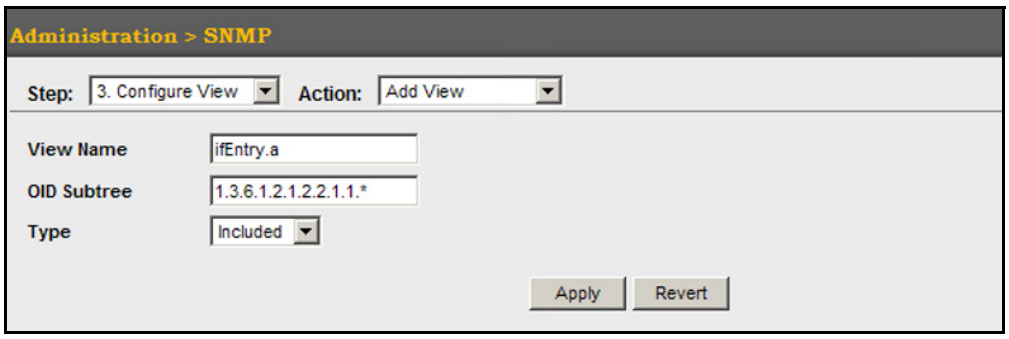
- **View Name** – Lists the SNMP views configured in the Add View page.
- **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

WEB INTERFACE

To configure an SNMP view of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Add View from the Action list.
4. Enter a view name and specify the initial OID subtree in the switch's MIB database to be included or excluded in the view. Use the Add OID Subtree page to add additional object identifier branches to the view.
5. Click Apply

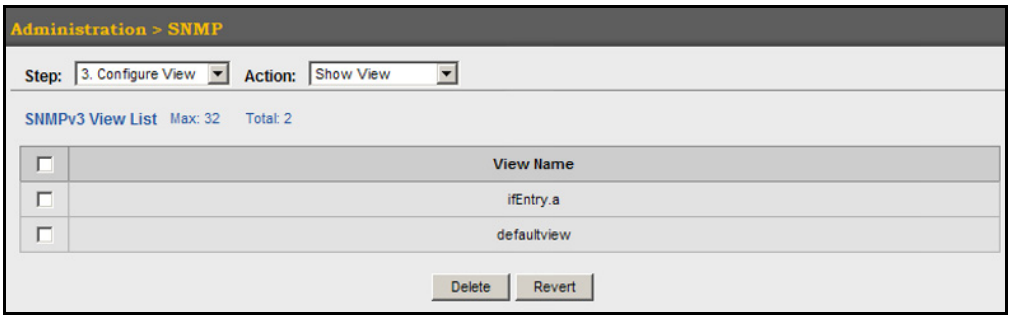
Figure 136: Creating an SNMP View



To show the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show View from the Action list.

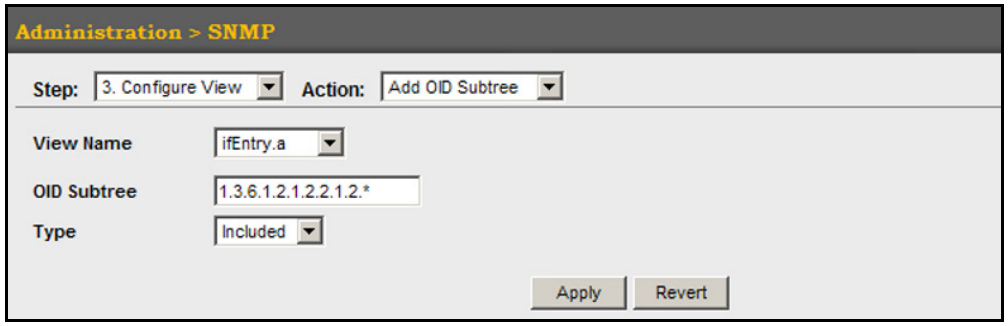
Figure 137: Showing SNMP Views



To add an object identifier to an existing SNMP view of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Add OID Subtree from the Action list.
4. Select a view name from the list of existing views, and specify an additional OID subtree in the switch's MIB database to be included or excluded in the view.
5. Click Apply

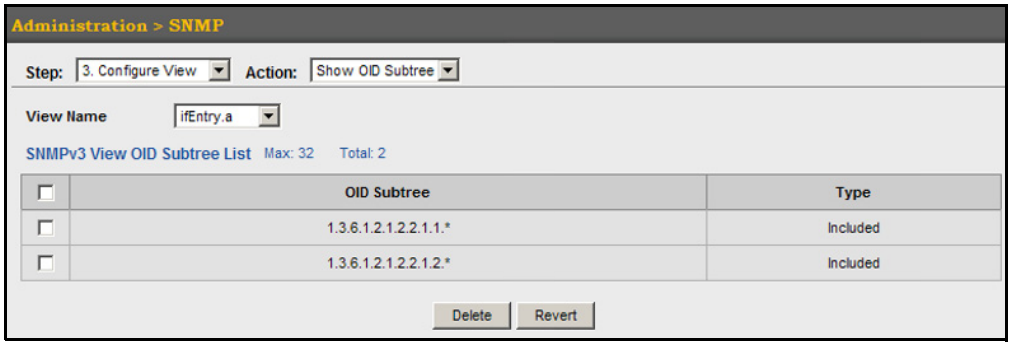
Figure 138: Adding an OID Subtree to an SNMP View



To show the OID branches configured for the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show OID Subtree from the Action list.
4. Select a view name from the list of existing views.

Figure 139: Showing the OID Subtree Configured for SNMP Views



CONFIGURING SNMPV3 GROUPS

Use the Administration > SNMP (Configure Group) page to add an SNMPv3 group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

PARAMETERS

These parameters are displayed:

- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Read View** – The configured view for read access. (Range: 1-64 characters)
- **Write View** – The configured view for write access. (Range: 1-64 characters)
- **Notify View** – The configured view for notifications. (Range: 1-64 characters)

Table 26: Supported Notification Messages

Model	Level	Group
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.

Table 26: Supported Notification Messages (Continued)

Model	Level	Group
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.
Private Traps		
swPowerStatus ChangeTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.1	This trap is sent when the power state changes.
swPortSecurityTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.
swIpFilterRejectTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swAuthenticationFailure	1.3.6.1.4.1.572.17389.12000.2.1.0.66	This trap will be triggered if authentication fails.
swAuthenticationSuccess	1.3.6.1.4.1.572.17389.12000.2.1.0.67	This trap will be triggered if authentication is successful.

Table 26: Supported Notification Messages (Continued)

Model	Level	Group
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.70	When broadcast traffic is detected as a storm, this trap is fired.
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.71	When a broadcast storm is detected as normal traffic, this trap is fired.
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.72	When ATC is activated, this trap is fired.
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.73	When ATC is released, this trap is fired.
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.74	When multicast traffic is detected as the storm, this trap is fired.
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.75	When multicast storm is detected as normal traffic, this trap is fired.
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.76	When ATC is activated, this trap is fired.
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.77	When ATC is released, this trap is fired.
stpBecomeRootBridgeTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.86	The stpBecomeRootBridge trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after it has been elected as the new root.
stpPortEnterForwardingTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.87	The trap is sent by a bridge when any of its configured ports transit from Learning state to Forwarding state.
stpRootPortChangedTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.88	The trap is sent when the root port of a bridge has changed.
stpRootBridgeChangedTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.89	The trap will be sent when the root bridge of bridges has changed and the bridge sending off the trap is not the root in STP topology.
swLoopbackDetectionTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.92	This trap is sent when loopback BPDUs have been detected.
autoUpgradeTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.104	This trap is sent when auto upgrade is executed.
swCpuUtiRisingNotification	1.3.6.1.4.1.572.17389.12000.2.1.0.107	This notification indicates that the CPU utilization has risen from cpuUtiFallingThreshold to cpuUtiRisingThreshold.
swCpuUtiFallingNotification	1.3.6.1.4.1.572.17389.12000.2.1.0.108	This notification indicates that the CPU utilization has fallen from cpuUtiRisingThreshold to cpuUtiFallingThreshold.
swMemoryUtiRisingThresholdNotification	1.3.6.1.4.1.572.17389.12000.2.1.0.109	This notification indicates that the memory utilization has risen from memoryUtiFallingThreshold to memoryUtiRisingThreshold.
swMemoryUtiFallingThresholdNotification	1.3.6.1.4.1.572.17389.12000.2.1.0.110	This notification indicates that the memory utilization has fallen from memoryUtiRisingThreshold to memoryUtiFallingThreshold.
dhcpRougeServerAttackTrap	1.3.6.1.4.1.572.17389.12000.2.1.0.114	This trap is sent when receiving a DHCP packet from a rouge server.

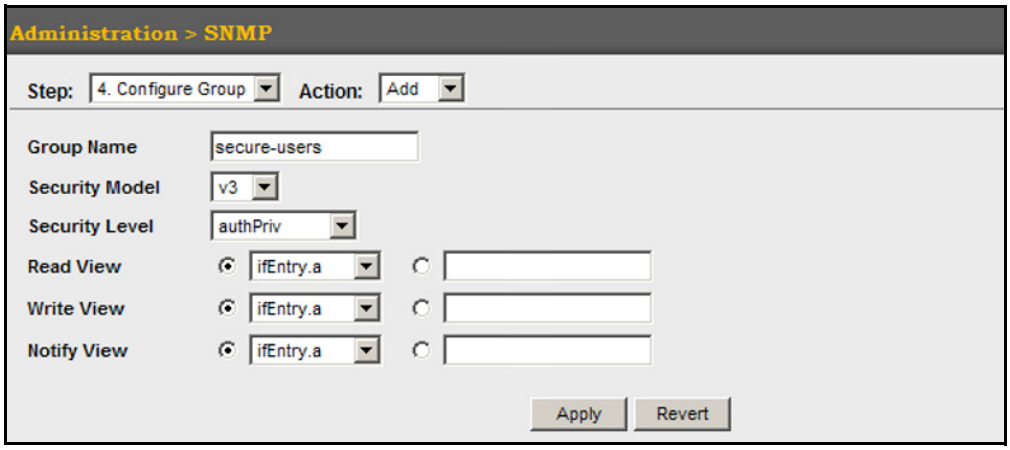
* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

WEB INTERFACE

To configure an SNMP group:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Enter a group name, assign a security model and level, and then select read, write, and notify views.
5. Click Apply

Figure 140: Creating an SNMP Group



To show SNMP groups:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 141: Showing SNMP Groups


Administration > SNMP
Step: 4. Configure Group
Action: Show
SNMPv3 Group List Max: 26 Total: 5
Group Name | Model | Level | Read View | Write View | Notify View
public | v1 | noAuthNoPriv | defaultview | No writeview specified | No notifyview specified
public | v2c | noAuthNoPriv | defaultview | No writeview specified | No notifyview specified
private | v1 | noAuthNoPriv | defaultview | defaultview | No notifyview specified
private | v2c | noAuthNoPriv | defaultview | defaultview | No notifyview specified
secure-users | v3 | authPriv | ifEntry.a | ifEntry.a | ifEntry.a
Delete
Revert

SETTING COMMUNITY ACCESS STRINGS

Use the Administration > SNMP (Configure User - Add Community) page to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

PARAMETERS

These parameters are displayed:

- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

  Range: 1-32 characters, case sensitive
  Default strings: "public" (Read-Only), "private" (Read/Write)

- **Access Mode** – Specifies the access rights for the community string:

  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.

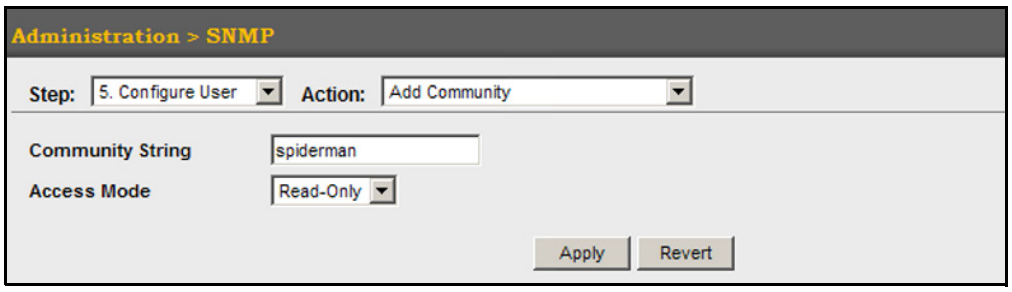
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

WEB INTERFACE

To set a community access string:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add Community from the Action list.
4. Add new community strings as required, and select the corresponding access rights from the Access Mode list.
5. Click Apply

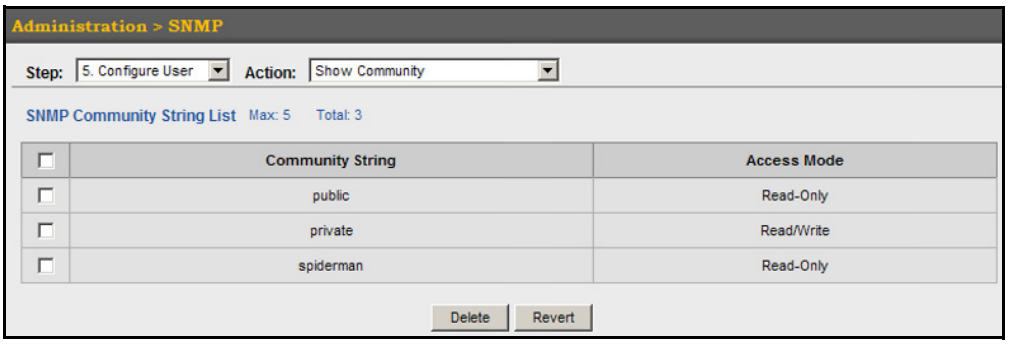
Figure 142: Setting Community Access Strings



To show the community access strings:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show Community from the Action list.

Figure 143: Showing Community Access Strings



CONFIGURING LOCAL SNMPV3 USERS

Use the Administration > SNMP (Configure User - Add SNMPv3 Local User) page to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

PARAMETERS

These parameters are displayed:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.

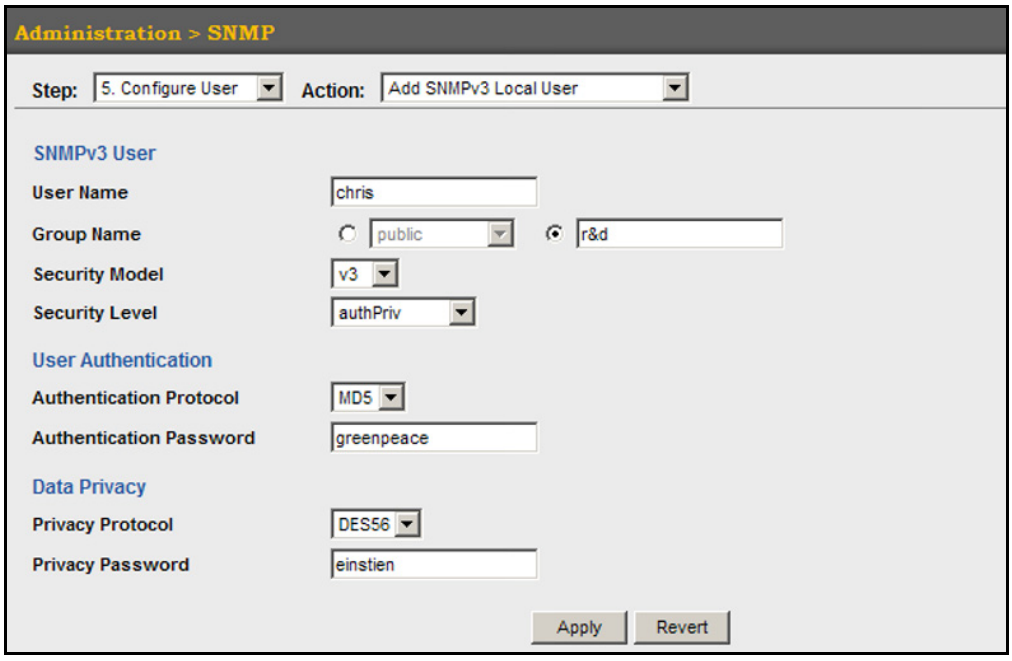
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a local SNMPv3 user:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add SNMPv3 Local User from the Action list.
4. Enter a name and assign it to a group. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
5. Click Apply

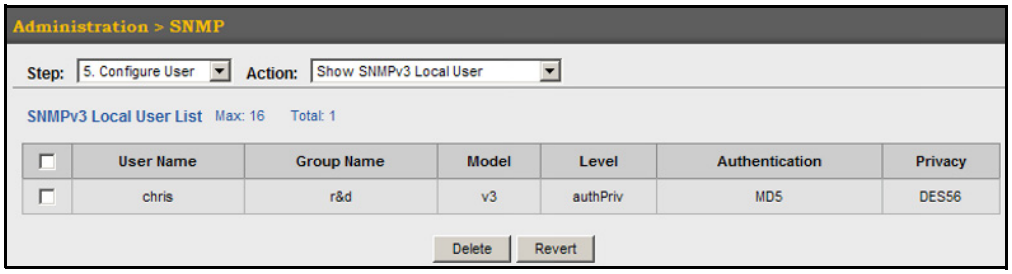
Figure 144: Configuring Local SNMPv3 Users



To show local SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Local User from the Action list.

Figure 145: Showing Local SNMPv3 Users



CONFIGURING REMOTE SNMPV3 USERS

Use the Administration > SNMP (Configure User - Add SNMPv3 Remote User) page to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

COMMAND USAGE

- To grant management access to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and the remote user. (See "Specifying Trap Managers" on page 245 and "Specifying a Remote Engine ID" on page 232.)

PARAMETERS

These parameters are displayed:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Remote IP** – The Internet address of the remote device where the user resides.
- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:

- **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
- **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
- **AuthPriv** – SNMP communications use both authentication and encryption.

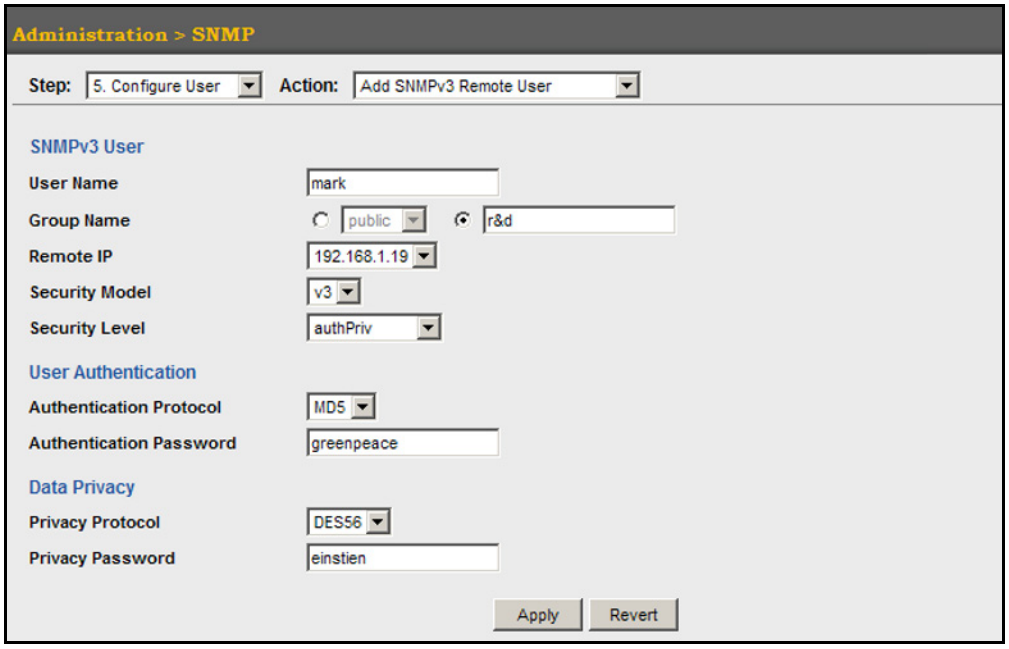
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a remote SNMPv3 user:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add SNMPv3 Remote User from the Action list.
4. Enter a name and assign it to a group. Enter the IP address to identify the source of SNMPv3 inform messages sent from the local switch. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
5. Click Apply

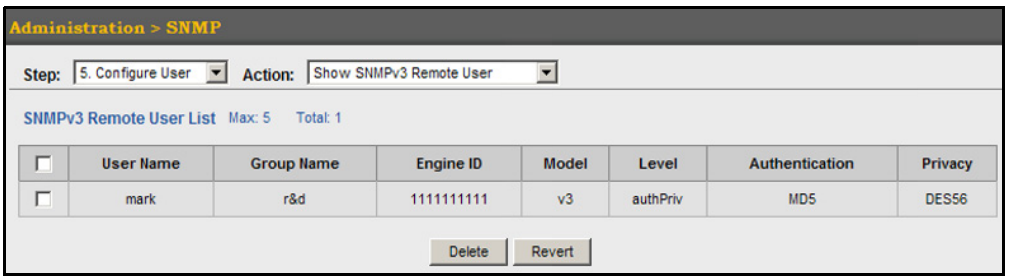
Figure 146: Configuring Remote SNMPv3 Users



To show remote SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Remote User from the Action list.

Figure 147: Showing Remote SNMPv3 Users



SPECIFYING TRAP MANAGERS

Use the Administration > SNMP (Configure Trap) page to specify the host devices to be sent traps and the types of traps to send. Traps indicating status changes are issued by the switch to the specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

COMMAND USAGE

- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch.

Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent (page 230).
2. Create a view with the required notification messages (page 233).
3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view (page 236).
4. Enable trap informs as described in the following pages.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 230).
2. Create a local SNMPv3 user to use in the message exchange process (page 241). If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified local user, and default settings for the read, write, and notify view.
3. Create a view with the required notification messages (page 233).
4. Create a group that includes the required notify view (page 236).
5. Enable trap informs as described in the following pages.

PARAMETERS

These parameters are displayed:

SNMP Version 1

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

  Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 2c

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).

- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- **Notification Type**
  - **Traps** – Notifications are sent as trap messages.
  - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
    - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
    - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

  Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 3

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- **Notification Type**
  - **Traps** – Notifications are sent as trap messages.
  - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
    - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
    - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

- **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch. (Range: 1-32 characters)

  If an account for the specified user has not been created (page 241), one will be automatically generated.

- **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters)

  If an account for the specified user has not been created (page 243), one will be automatically generated.

- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

- **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)

  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.

  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.

  - **AuthPriv** – SNMP communications use both authentication and encryption.

WEB INTERFACE

To configure trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Add from the Action list.
4. Fill in the required parameters based on the selected SNMP version.
5. Click Apply

Figure 148: Configuring Trap Managers (SNMPv1)

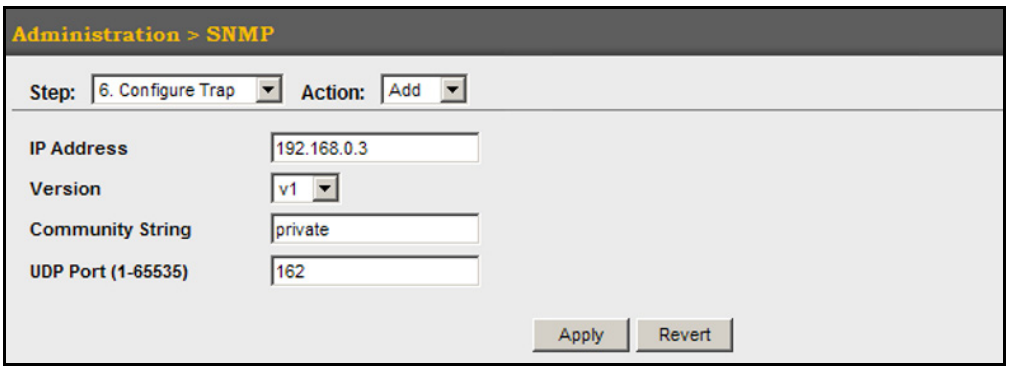


Figure 149: Configuring Trap Managers (SNMPv2c)

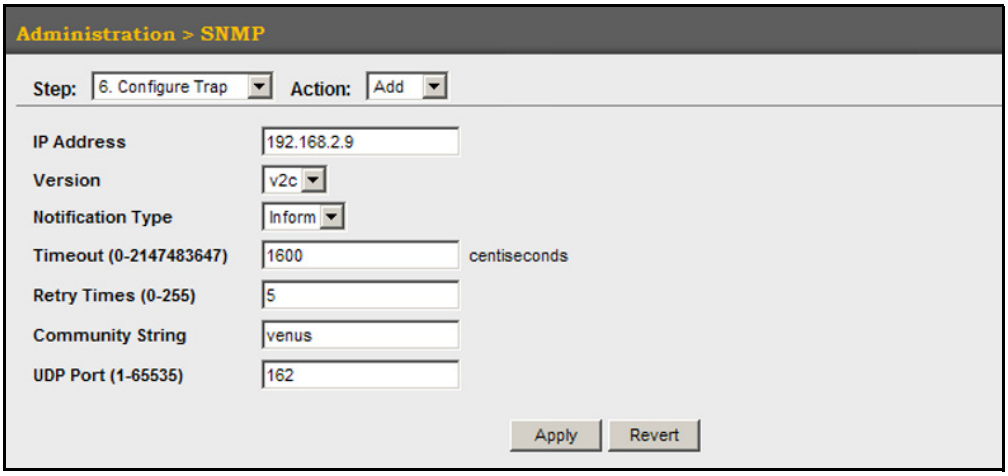
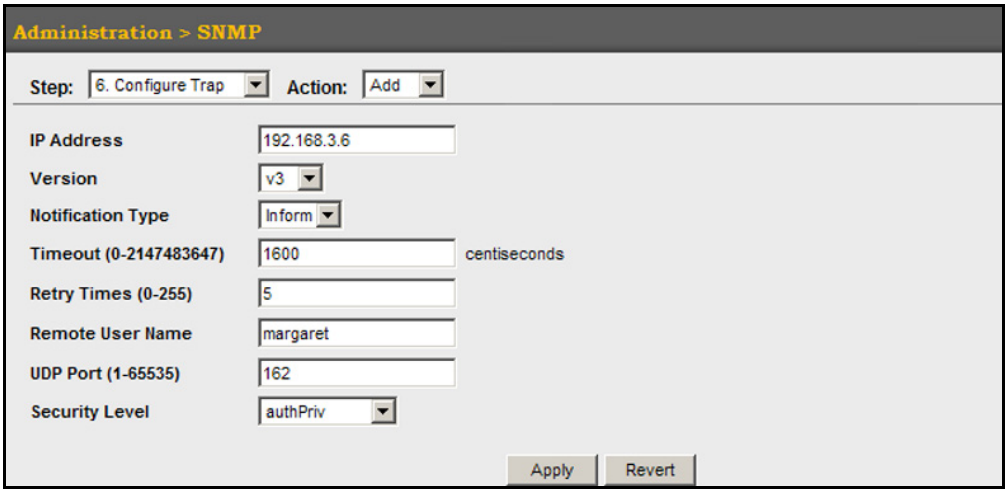


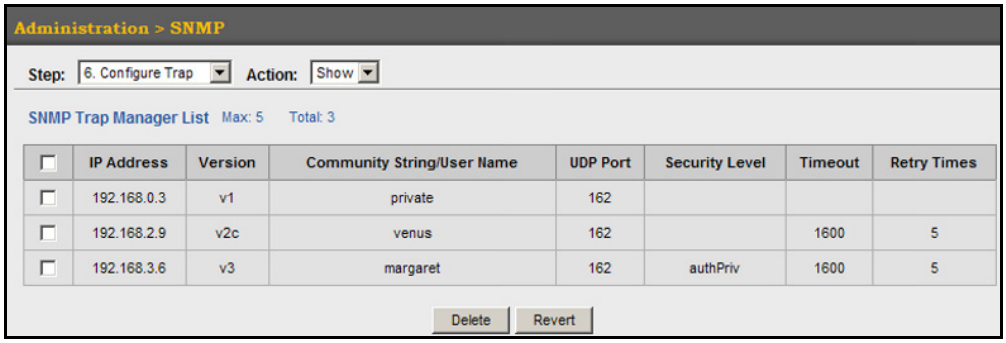
Figure 150: Configuring Trap Managers (SNMPv3)



To show configured trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Show from the Action list.

Figure 151: Showing Trap Managers



REMOTE MONITORING

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

The switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

CONFIGURING RMON ALARMS

Use the Administration > RMON (Configure Global - Add - Alarm) page to define specific criteria that will generate response events. Alarms can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to rising or falling thresholds. (However, note that after an alarm is triggered it will not be triggered again until the statistical

value crosses the opposite bounding threshold and then back across the trigger threshold.

COMMAND USAGE

- If an alarm is already defined for an index, the entry must be deleted before any changes can be made.

PARAMETERS

These parameters are displayed:

- **Index** – Index to this entry. (Range: 1-65535)
- **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled.

  Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.
- **Interval** – The polling interval. (Range: 1-31622400 seconds)
- **Sample Type** – Tests for absolute or relative changes in the specified variable.
  - **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.
  - **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.
- **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. (Range: 1-65535)
- **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)
- **Falling Threshold** – If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: 1-65535)
- **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling

threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

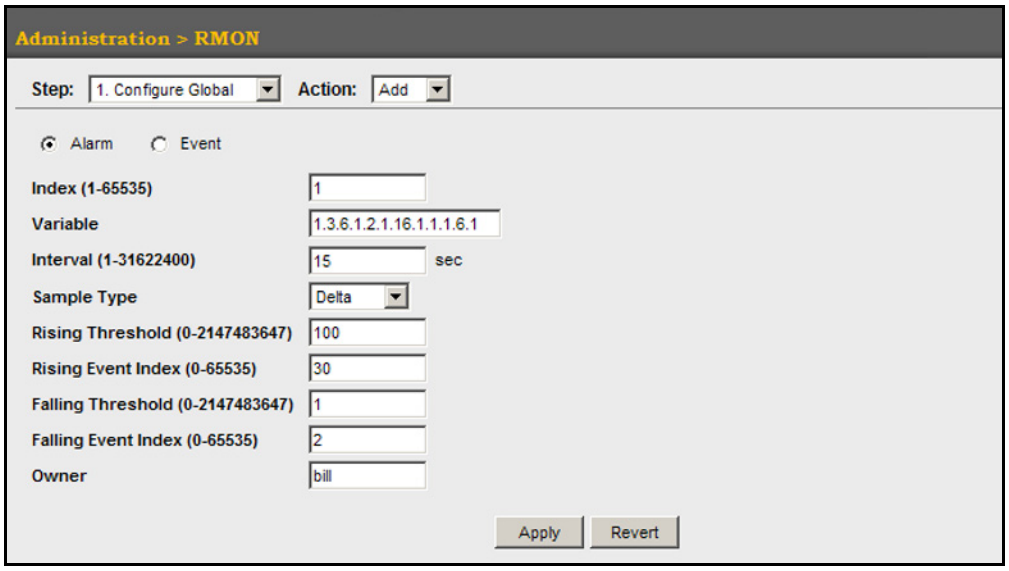
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON alarm:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Alarm.
5. Enter an index number, the MIB object to be polled (etherStatsEntry.n.n), the polling interval, the sample type, the thresholds, and the event to trigger.
6. Click Apply

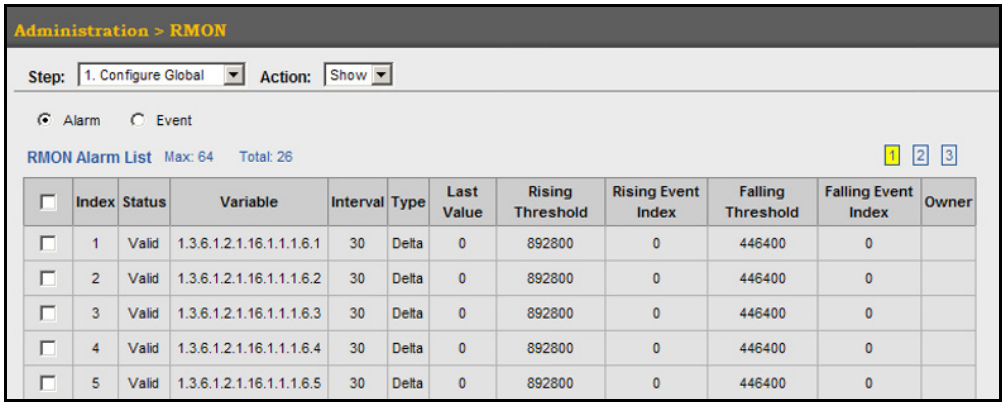
Figure 152: Configuring an RMON Alarm



To show configured RMON alarms:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Alarm.

Figure 153: Showing Configured RMON Alarms



Index	Status	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
1	Valid	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
5	Valid	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	

CONFIGURING RMON EVENTS

Use the Administration > RMON (Configure Global - Add - Event) page to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

COMMAND USAGE

- If an alarm is already defined for an index, the entry must be deleted before any changes can be made.
- One default event is configured as follows:

  event Index = 1
  Description: RMON_TRAP_LOG
  Event type: log & trap
  Event community name is public
  Owner is RMON_SNMP

PARAMETERS

These parameters are displayed:

- **Index** – Index to this entry. (Range: 1-65535)
- **Type** – Specifies the type of event to initiate:
  - **None** – No event is generated.
  - **Log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see "System Log Configuration" on page 201).
  - **Trap** – Sends a trap message to all configured trap managers (see "Specifying Trap Managers" on page 245).
  - **Log and Trap** – Logs the event and sends a trap message.

- **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts.

  Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page (see "Setting Community Access Strings" on page 240) prior to configuring it here. (Range: 1-127 characters)

- **Description** – A comment that describes this event. (Range: 1-127 characters)

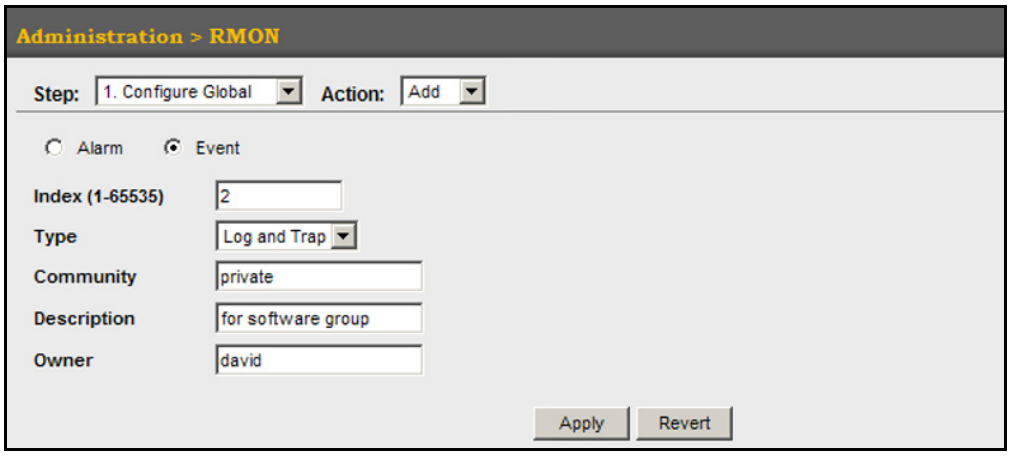
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON event:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Event.
5. Enter an index number, the type of event to initiate, the community string to send with trap messages, the name of the person who created this event, and a brief description of the event.
6. Click Apply

Figure 154: Configuring an RMON Event



To show configured RMON events:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Event.

Figure 155: Showing Configured RMON Events



CONFIGURING RMON HISTORY SAMPLES

Use the Administration > RMON (Configure Interface - Add - History) page to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems. The record can be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. It can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

COMMAND USAGE

- Each index number equates to a port on the switch.
- If history collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- The information collected for each sample includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.

  For a description of the statistics displayed on the Show Details page, refer to "Showing Port or Trunk Statistics" on page 71.

PARAMETERS

These parameters are displayed:

- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)

- **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800 seconds)
- **Buckets** - The number of buckets requested for this entry. (Range: 1-65536; Default: 50)

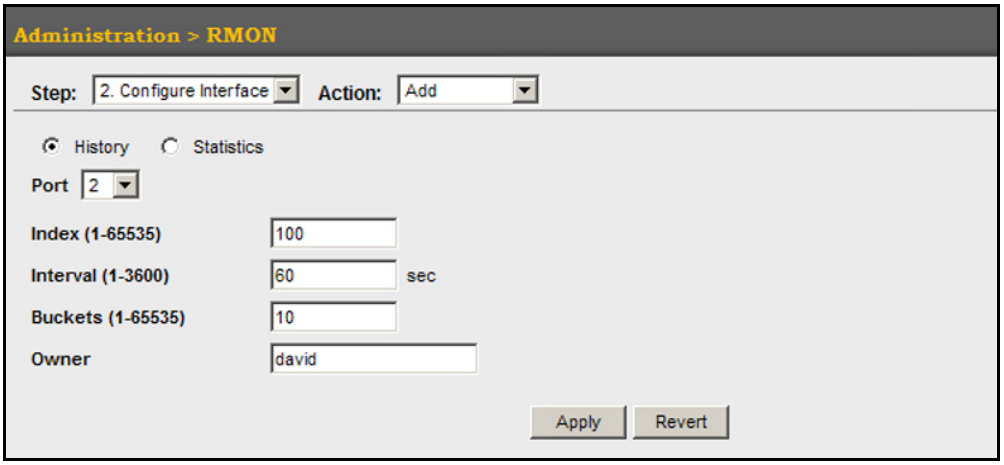
  The number of buckets granted are displayed on the Show page.
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To periodically sample statistics on a port:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click History.
5. Select a port from the list as the data source.
6. Enter an index number, the sampling interval, the number of buckets to use, and the name of the owner for this entry.
7. Click Apply

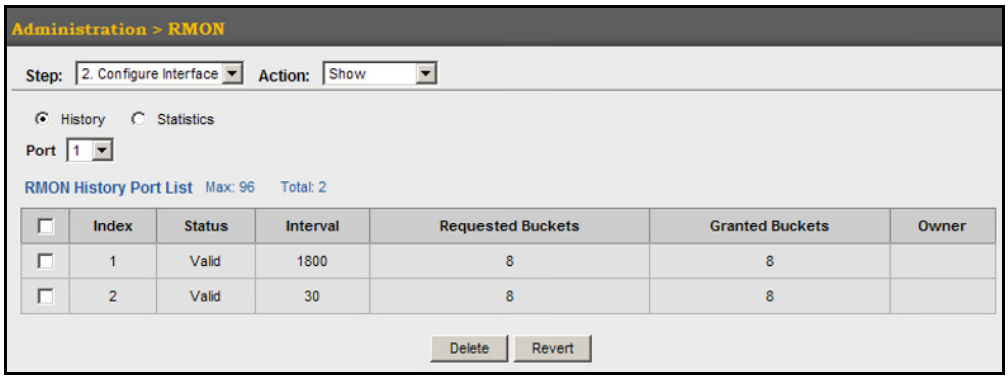
Figure 156: Configuring an RMON History Sample



To show configured RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port from the list.
5. Click History.

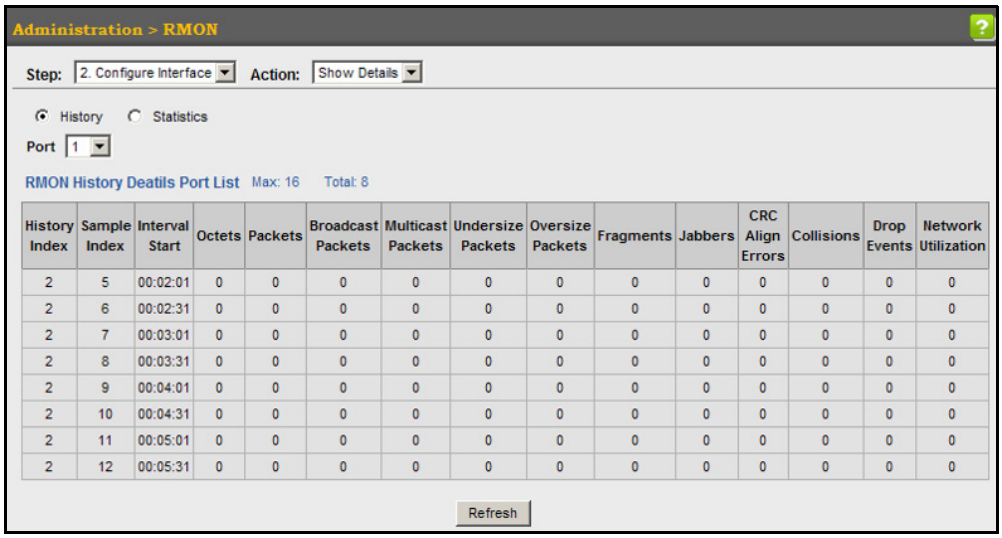
Figure 157: Showing Configured RMON History Samples



To show collected RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.
4. Select a port from the list.
5. Click History.

Figure 158: Showing Collected RMON History Samples



History Index	Sample Index	Interval Start	Octets	Packets	Broadcast Packets	Multicast Packets	Undersize Packets	Oversize Packets	Fragments	Jabbers	CRC Align Errors	Collisions	Drop Events	Network Utilization
2	5	00:02:01	0	0	0	0	0	0	0	0	0	0	0	0
2	6	00:02:31	0	0	0	0	0	0	0	0	0	0	0	0
2	7	00:03:01	0	0	0	0	0	0	0	0	0	0	0	0
2	8	00:03:31	0	0	0	0	0	0	0	0	0	0	0	0
2	9	00:04:01	0	0	0	0	0	0	0	0	0	0	0	0
2	10	00:04:31	0	0	0	0	0	0	0	0	0	0	0	0
2	11	00:05:01	0	0	0	0	0	0	0	0	0	0	0	0
2	12	00:05:31	0	0	0	0	0	0	0	0	0	0	0	0

CONFIGURING RMON STATISTICAL SAMPLES

Use the Administration > RMON (Configure Interface - Add - Statistics) page to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates.

COMMAND USAGE

- If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- The information collected for each entry includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

PARAMETERS

These parameters are displayed:

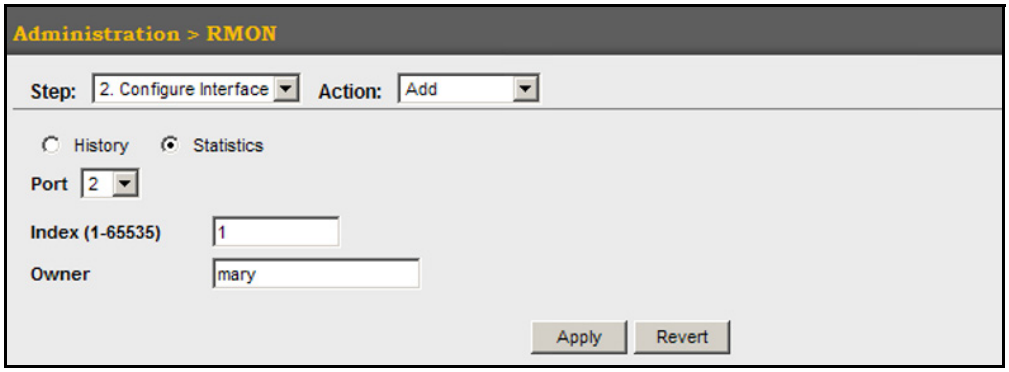
- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To enable regular sampling of statistics on a port:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click Statistics.
5. Select a port from the list as the data source.
6. Enter an index number, and the name of the owner for this entry
7. Click Apply

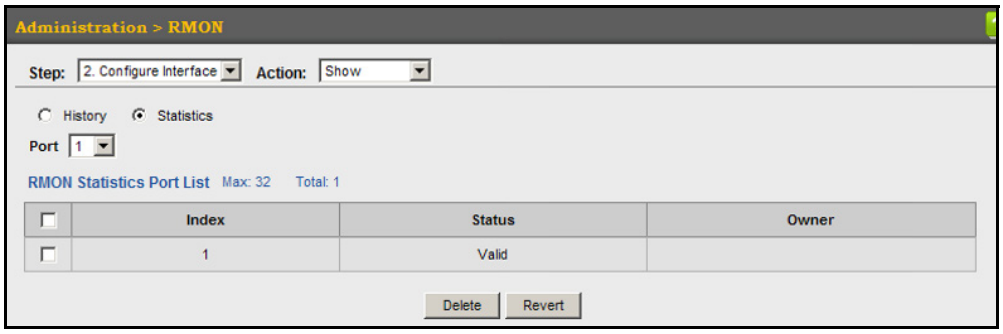
Figure 159: Configuring an RMON Statistical Sample



To show configured RMON statistical samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port from the list.
5. Click Statistics.

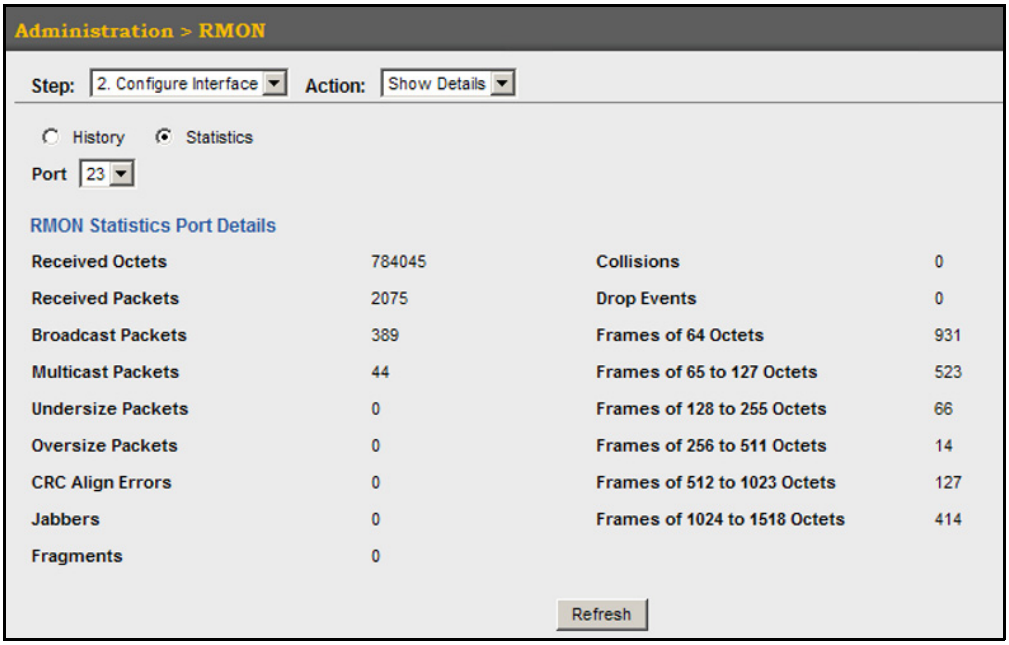
Figure 160: Showing Configured RMON Statistical Samples



To show collected RMON statistical samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.
4. Select a port from the list.
5. Click Statistics.

Figure 161: Showing Collected RMON Statistical Samples



SWITCH CLUSTERING

Switch clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

COMMAND USAGE

- A switch cluster has a "Commander" unit that is used to manage all other "Member" switches in the cluster. The management station can use the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage Member switches using the cluster's "internal" IP addresses.
- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.
- There can be up to 100 candidates and 36 member switches in one cluster.
- A switch can only be a member of one cluster.
- The cluster VLAN 4093 is not configured by default. Before using clustering, take the following actions to set up this VLAN:
  1. Create VLAN 4093 (see "Configuring VLAN Groups" on page 95).
  2. Add the participating ports to this VLAN (see "Adding Static Members to VLANs" on page 96), and set them to hybrid mode, tagged members, PVID = 1, and acceptable frame type = all.
- After the Commander and Members have been configured, any switch in the cluster can be managed from the web agent by choosing the desired Member ID from the Show Member page.

CONFIGURING GENERAL SETTINGS FOR CLUSTERS

Use the Administration > Cluster (Configure Global) page to create a switch cluster.

COMMAND USAGE

First be sure that clustering is enabled on the switch (the default is disabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

PARAMETERS

These parameters are displayed:

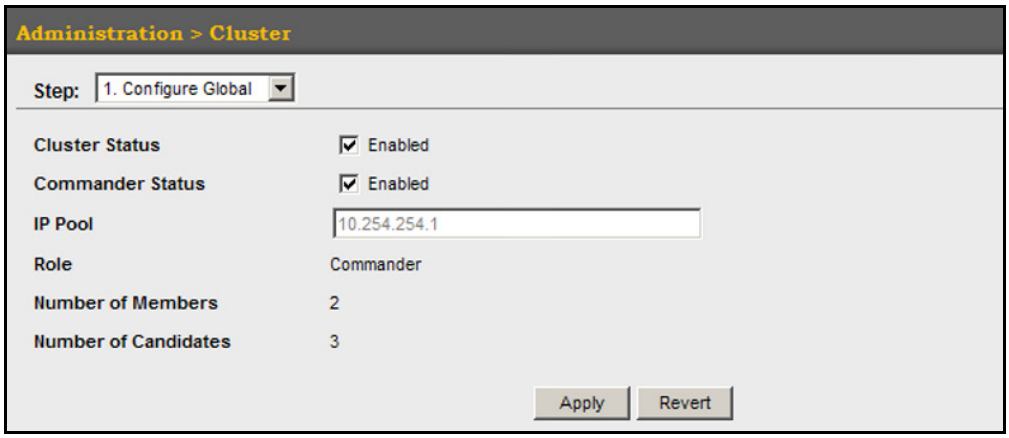
- **Cluster Status** – Enables or disables clustering on the switch. (Default: Disabled)
- **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- **IP Pool** – An "internal" IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)
- **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate. (Default: Candidate)
- **Number of Members** – The current number of Member switches in the cluster.
- **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

WEB INTERFACE

To configure a switch cluster:

1. Click Administration, Cluster.
2. Select Configure Global from the Step list.
3. Set the required attributes for a Commander or a managed candidate.
4. Click Apply

Figure 162: Configuring a Switch Cluster



CLUSTER MEMBER CONFIGURATION

Use the Administration > Cluster (Configure Member - Add) page to add Candidate switches to the cluster as Members.

PARAMETERS

These parameters are displayed:

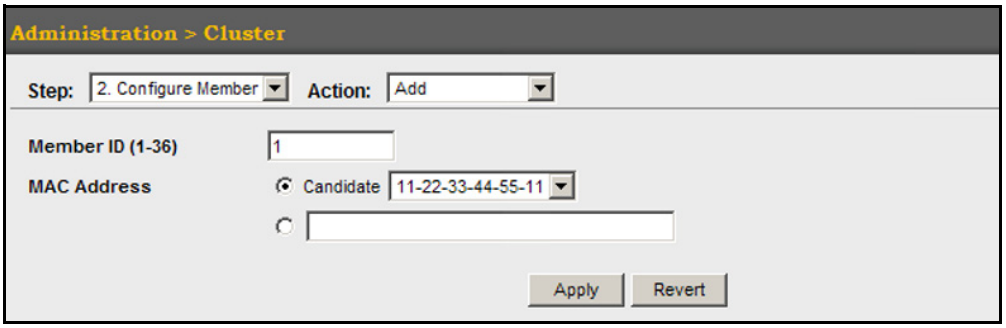
- **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

WEB INTERFACE

To configure cluster members:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Add from the Action list.
4. Select one of the cluster candidates discovered by this switch, or enter the MAC address of a candidate.
5. Click Apply.

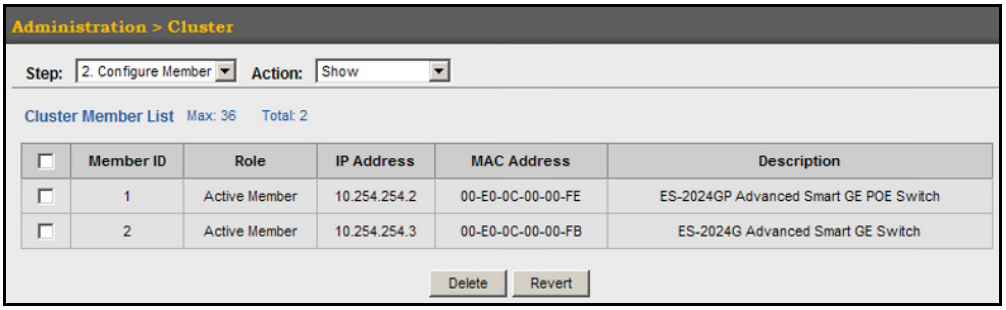
Figure 163: Configuring a Cluster Members



To show the cluster members:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Show from the Action list.

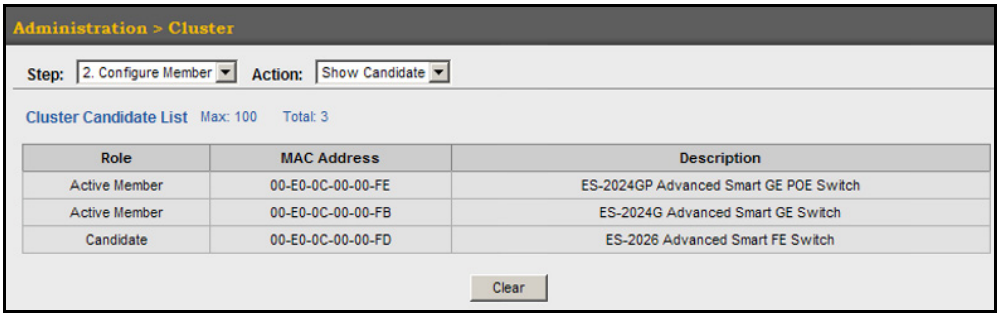
Figure 164: Showing Cluster Members



To show cluster candidates:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Show Candidate from the Action list.

Figure 165: Showing Cluster Candidates



MANAGING CLUSTER MEMBERS

Use the Administration > Cluster (Show Member) page to manage another switch in the cluster.

PARAMETERS

These parameters are displayed:

Member ID – The ID number of the Member switch. (Range: 1-36)

Role – Indicates the current status of the switch in the cluster.

IP Address – The internal cluster IP address assigned to the Member switch.

MAC Address – The MAC address of the Member switch.

Description – The system description string of the Member switch.

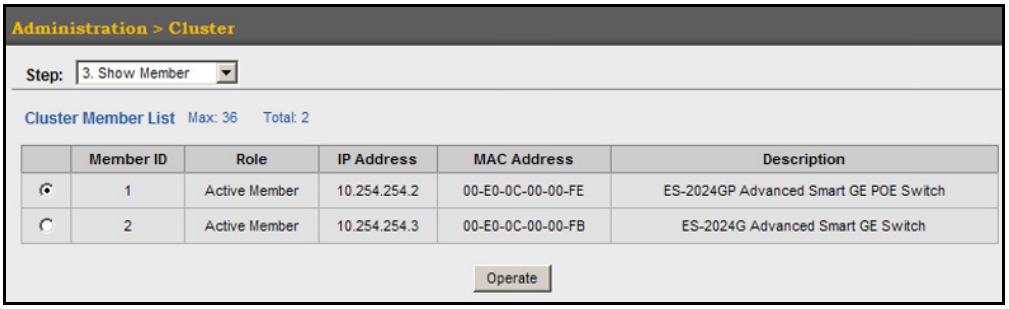
Operate – Remotely manage a cluster member.

WEB INTERFACE

To manage a cluster member:

1. Click Administration, Cluster.
2. Select Show Member from the Step list.
3. Select an entry from the Cluster Member List.
4. Click Operate.

Figure 166: Managing a Cluster Member



16 IP CONFIGURATION

This chapter describes how to configure an IP interface for management access to the switch over the network. You can manually configure a specific IP address or direct the switch to obtain an address from a BOOTP or DHCP server when it is powered on.

This chapter provides information on network functions including:

- Ping – Sends ping message to another node on the network.
- Address Resolution Protocol – Specifies the timeout for ARP cache entries. Also shows how to display the ARP cache.
- IP Configuration – Sets an IP address for management access.

USING THE PING FUNCTION

Use the IP > General > Ping page to send ICMP echo request packets to another node on the network.

PARAMETERS

These parameters are displayed:

- **IP Address** – IP address of the host.
- **Probe Count** – Number of packets to send. (Range: 1-16)
- **Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes)

  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

COMMAND USAGE

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.

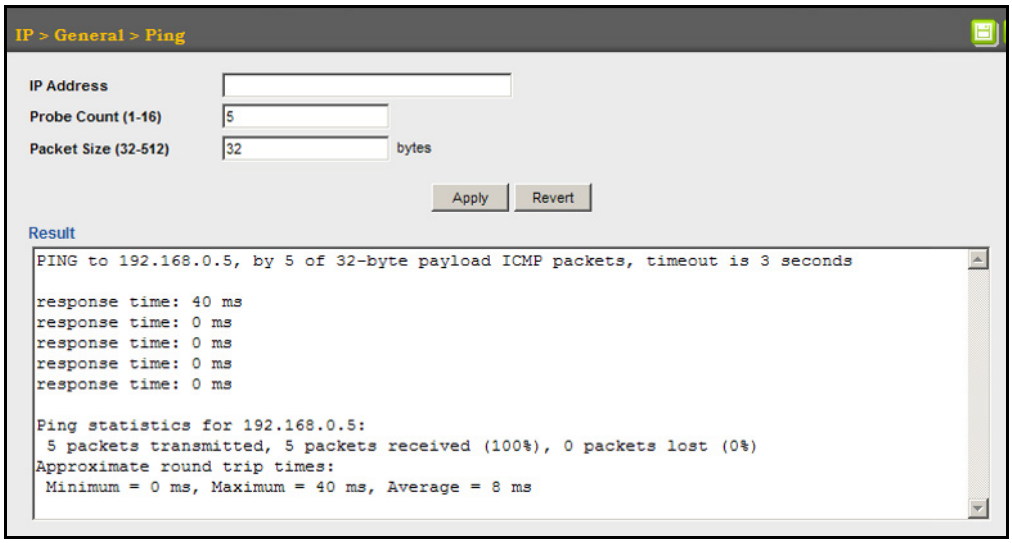
- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table.

WEB INTERFACE

To ping another device on the network:

1. Click IP, General, Ping.
2. Specify the target device and ping parameters.
3. Click Apply.

Figure 167: Pinging a Network Device


IP > General > Ping
IP Address
Probe Count (1-16)
5
Packet Size (32-512)
32
bytes
Apply
Revert
Result
PING to 192.168.0.5, by 5 of 32-byte payload ICMP packets, timeout is 3 seconds
response time: 40 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
Ping statistics for 192.168.0.5:
5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
Minimum = 0 ms, Maximum = 40 ms, Average = 8 ms

ADDRESS RESOLUTION PROTOCOL

Address Resolution Protocol (ARP) is used to map an IP address to a physical layer (i.e., MAC) address. When a device sends or receives a packet with an IP header, it must first resolve the destination IP address into a MAC address. When an IP frame is received by this switch, it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the switch writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the destination.

If there is no entry for an IP address in the ARP cache, the switch will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

Table 27: Address Resolution Protocol

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the switch will be able forward traffic directly to the next hop without having to broadcast another ARP request.

Also, if the switch receives a request for its own IP address, it will send back a response, and also cache the MAC of the source device's IP address.

SETTING THE ARP TIMEOUT

Use the IP > ARP (Configure General) page to specify the timeout for ARP cache entries.

PARAMETERS

These parameters are displayed:

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)

  The ARP aging timeout can only be set globally for all VLANs.

  The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the switch may tie up resources by repeating ARP requests for addresses recently flushed from the table.

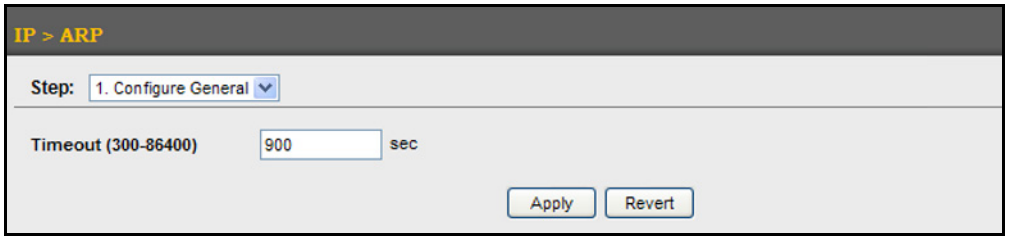
  When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

WEB INTERFACE

To configure the timeout for the ARP cache or to enable Proxy ARP for a VLAN (i.e., IP subnetwork):

1. Click IP, ARP.
2. Select Configure General from the Step List.
3. Set the timeout to a suitable value for the ARP cache.
4. Click Apply.

Figure 168: Setting the ARP Timeout



DISPLAYING ARP ENTRIES

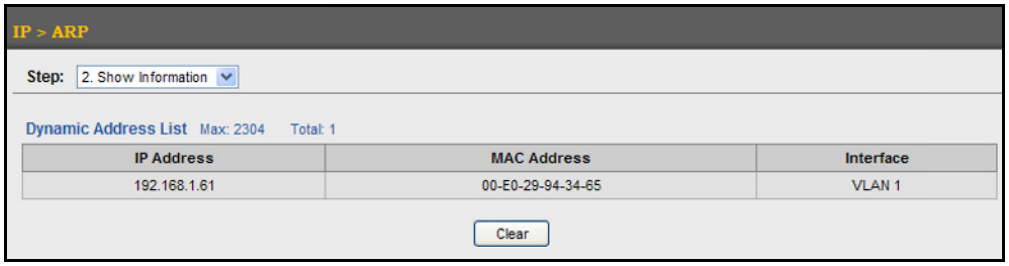
Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache. The ARP cache contains entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

WEB INTERFACE

To display entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.

Figure 169: Displaying ARP Entries



SETTING THE SWITCH'S IP ADDRESS (IP VERSION 4)

Use the System > IP page to configure an IPv4 address for management access over the network. You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

A static address of 192.168.1.10 is set by default for VLAN 1. To configure an address compatible with your network, you need to change the switch's default settings. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

PARAMETERS

These parameters are displayed:

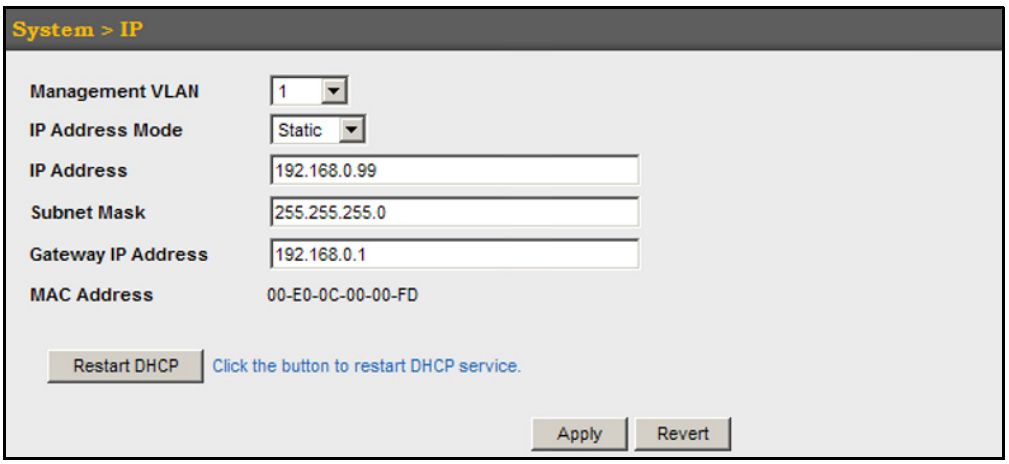
- **Management VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP values can include the IP address, subnet mask, and default gateway. (Default: Static)
- **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.1.10)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Gateway IP Address** – IP address of the gateway router between the switch and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.
- **Restart DHCP** – Requests a new IP address from the DHCP server.

WEB INTERFACE

To set a static address for the switch:

1. Click System, IP.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to "Static," enter the IP address, subnet mask and gateway.
3. Click Apply.

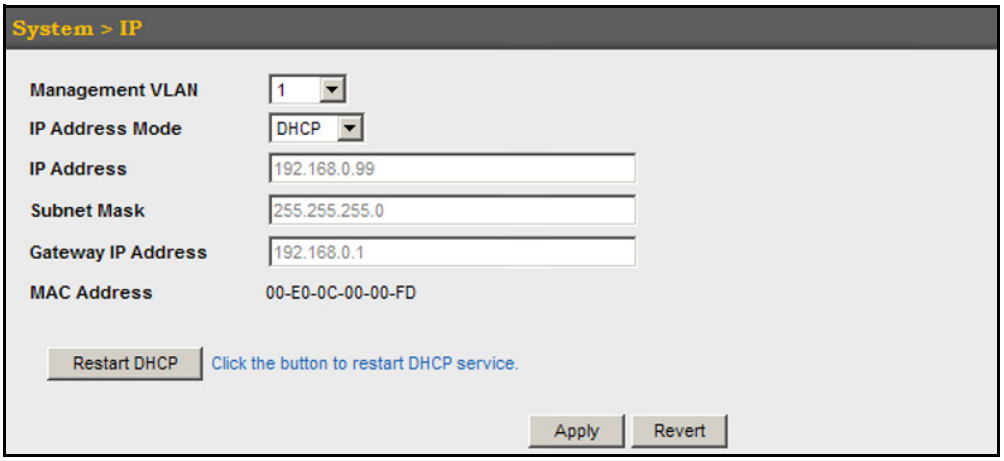
Figure 170: Configuring a Static IPv4 Address



To obtain an dynamic address through DHCP/BOOTP for the switch:

1. Click System, IP.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to "DHCP" or "BOOTP."
3. Click Apply to save your changes.
4. Then click Restart DHCP to immediately request a new address.

Figure 171: Configuring a Dynamic IPv4 Address



NOTE: The switch will also broadcast a request for IP configuration settings on each power reset.

NOTE: When using DHCP, you may lose the management connection if the IP address assigned by the DHCP server has changed. To resolve this kind of problem, ask your network administrator to configure a static binding for your switch's MAC address on the DHCP server.

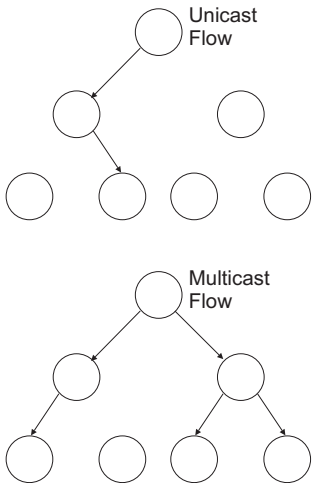
Renewing DHCP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch to restore the default static address.

If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

17 MULTICAST FILTERING

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

Figure 172: Multicast Filtering Concept



This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports

containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

LAYER 2 IGMP (SNOOPING AND QUERY)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 277) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering.

NOTE: When the switch is configured to use IGMPv2 snooping, the snooping version may be downgraded to version 1, depending on the version of the IGMP query packets detected on each VLAN.

NOTE: IGMP snooping will not function unless a multicast router port is enabled on the switch. This can accomplished in one of two ways. A static router port can be manually configured (see "Specifying Static Interfaces for a Multicast Router" on page 280). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

NOTE: A maximum of up to 255 multicast entries can be maintained for IGMP snooping. Once the table is full, no new entries are learned. Any subsequent multicast traffic not found in the table is dropped if unregistered-flooding is disabled (default behavior) and no router port is configured in the attached VLAN, or flooded throughout the VLAN if unregistered-flooding is enabled (see "Configuring IGMP Snooping and Query Parameters" on page 277).

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 280). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 282).

CONFIGURING IGMP SNOOPING AND QUERY PARAMETERS

Use the Multicast > IGMP Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

COMMAND USAGE

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

NOTE: If unknown multicast traffic enters a VLAN which has been configured with a router port, the traffic is forwarded to that port. However, if no router port exists on the VLAN, the traffic is dropped if unregistered-flooding is disabled (default behavior), or flooded throughout the VLAN if unregistered-flooding is enabled (see "Unregistered Data Flood" in the Command Attributes section).

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

NOTE: Multicast routers use this information from IGMP snooping and query reports, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

PARAMETERS

These parameters are displayed:

- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

  When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence (see "Setting IGMP Snooping Status per Interface" on page 284).

  When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

  When a spanning tree topology change occurs, the multicast membership information learned by switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, an switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with TC bit set (by the root bridge) will enter into "multicast flooding mode" for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

  If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a time out mechanism is used to delete all of the currently learned multicast channels.

  When a new uplink port starts up, the switch sends unsolicited reports for all currently learned channels out the new uplink port.

  By default, the switch immediately enters into "multicast flooding mode" when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive packet loss on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned. Otherwise, the time spent in flooding mode can be manually configured to reduce excessive loading.

  When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

  The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

- **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

  When the root bridge in a spanning tree receives a TCN for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (or query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it immediately issues an IGMP general query.

  A query solicitation can be sent whenever the switch notices a topology change, even if it is not the root bridge in spanning tree.

- **Router Alert Option** – Discards any IGMPv2 packets that do not include the Router Alert option. (Default: Disabled)

  As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common

method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option.

- **Unregistered Data Flooding** – Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled)

  Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

- **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

- **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. (Range: 1-65535 seconds, Default: 400 seconds)

  When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels via the new upstream interface.

  This command only applies when proxy reporting is enabled.

- **Router Port Expire Time** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)

- **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-2; Default: 2)

  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 2 are supported, and version 2 is backward compatible, so the switch can operate with other devices using either Version 1 or 2.

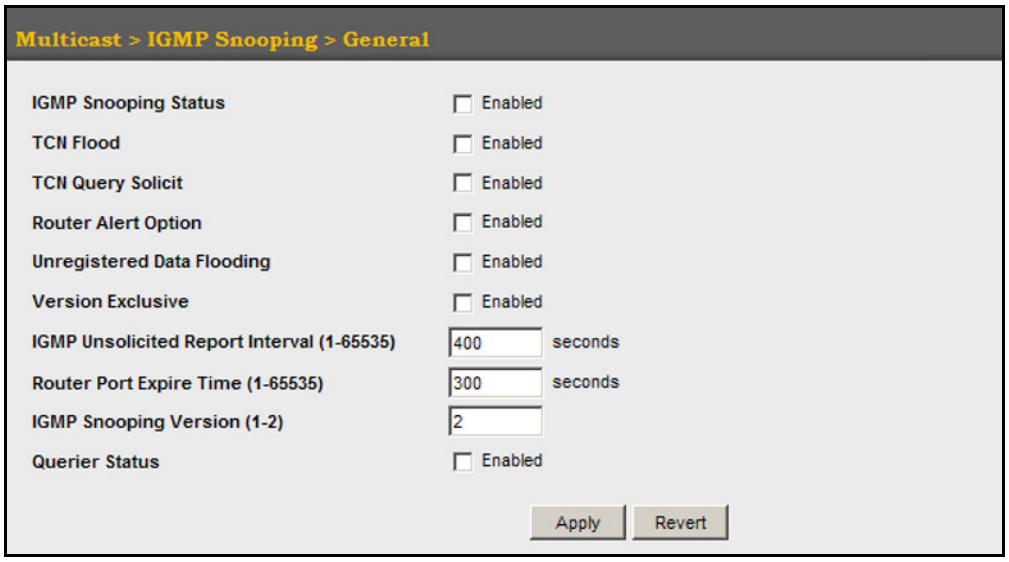
- **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

WEB INTERFACE

To configure general settings for IGMP Snooping and Query:

1. Click Multicast, IGMP Snooping, General.
2. Adjust the IGMP settings as required.
3. Click Apply.

Figure 173: Configuring General Settings for IGMP Snooping



SPECIFYING STATIC INTERFACES FOR A MULTICAST ROUTER

Use the Multicast > IGMP Snooping > Multicast Router (Add) page to statically attach an interface to a multicast router/switch.

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

PARAMETERS

These parameters are displayed:

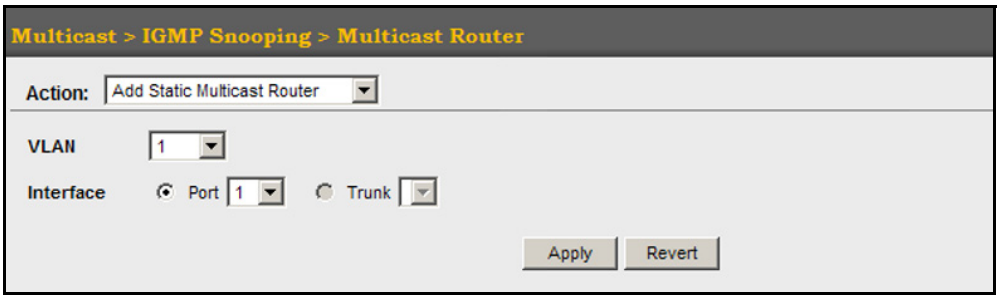
- **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

WEB INTERFACE

To specify a static interface attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Add Static Multicast Router from the Action list.
3. Select the VLAN which will forward all the corresponding multicast traffic, and select the port or trunk attached to the multicast router.
4. Click Apply.

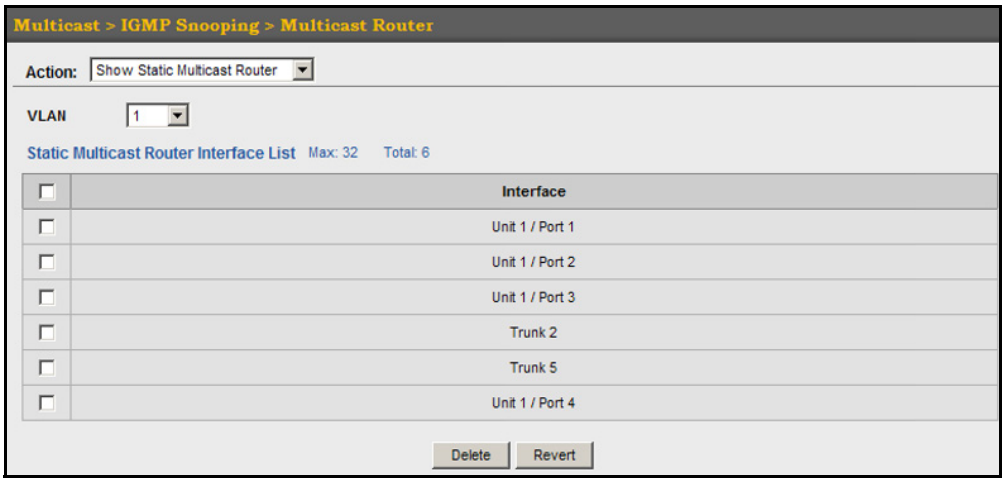
Figure 174: Configuring a Static Interface for a Multicast Router



To show the static interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Show Static Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

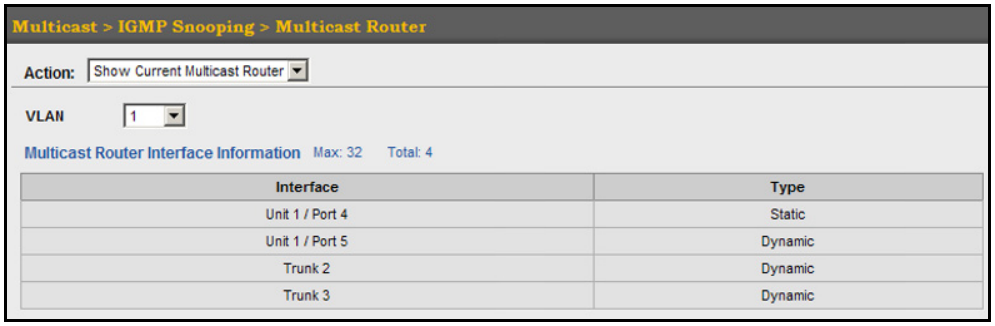
Figure 175: Showing Static Interfaces Attached a Multicast Router



To show the all interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Current Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 176: Showing Current Interfaces Attached a Multicast Router



ASSIGNING INTERFACES TO MULTICAST SERVICES

Use the Multicast > IGMP Snooping > IGMP Member (Add Static Member) page to statically assign a multicast service to an interface.

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages (see "Configuring IGMP Snooping and Query Parameters" on page 277). However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

COMMAND USAGE

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

PARAMETERS

These parameters are displayed:

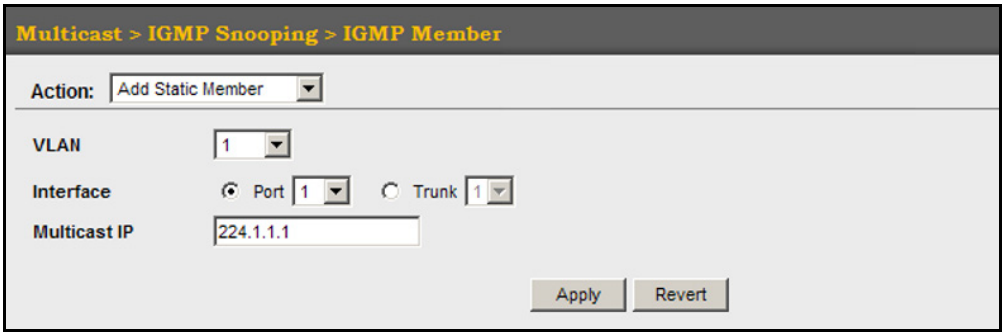
- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface assigned to a multicast group.
- **Multicast IP** – The IP address for a specific multicast service.

WEB INTERFACE

To statically assign an interface to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Add Static Member from the Action list.
3. Select the VLAN that will propagate the multicast service, specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), and enter the multicast IP address.
4. Click Apply.

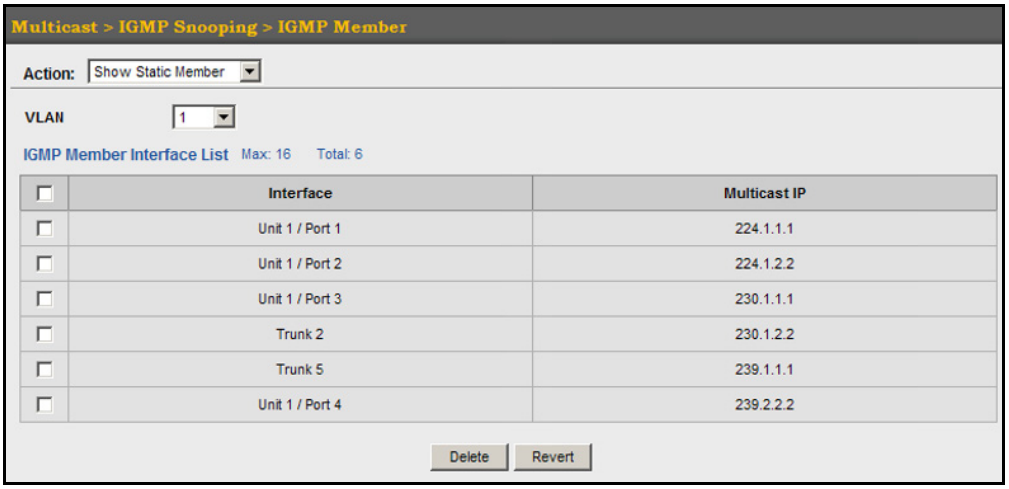
Figure 177: Assigning an Interface to a Multicast Service



To show the static interfaces assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Static Member from the Action list.
3. Select the VLAN for which to display this information.

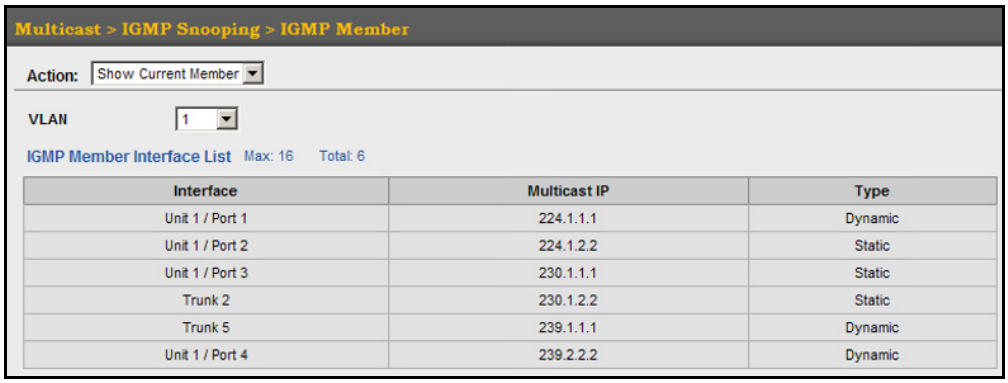
Figure 178: Showing Static Interfaces Assigned to a Multicast Service



To show the all interfaces statically or dynamically assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Current Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 179: Showing Current Interfaces Assigned to a Multicast Service


Multicast > IGMP Snooping > IGMP Member
Action: Show Current Member
VLAN 1
IGMP Member Interface List Max: 16 Total: 6
Interface | Multicast IP | Type
Unit 1 / Port 1 | 224.1.1.1 | Dynamic
Unit 1 / Port 2 | 224.1.2.2 | Static
Unit 1 / Port 3 | 230.1.1.1 | Static
Trunk 2 | 230.1.2.2 | Static
Trunk 5 | 239.1.1.1 | Dynamic
Unit 1 / Port 4 | 239.2.2.2 | Dynamic

SETTING IGMP SNOOPING STATUS PER INTERFACE

Use the Multicast > IGMP Snooping > Interface (Configure) page to configure IGMP snooping attributes for a VLAN interface. To configure snooping globally, refer to "Configuring IGMP Snooping and Query Parameters" on page 277.

COMMAND USAGE

Multicast Router Discovery

There have been many mechanisms used in the past to identify multicast routers. This has lead to interoperability issues between multicast routers and snooping switches from different vendors. In response to this problem, the Multicast Router Discovery (MRD) protocol has been developed for use by IGMP snooping and multicast routing devices. MRD is used to discover which interfaces are attached to multicast routers, allowing IGMP-enabled devices to determine where to send multicast source and group membership messages. (MRD is specified in draft-ietf-magma-mrdisc-07.)

Multicast source data and group membership reports must be received by all multicast routers on a segment. Using the group membership protocol query messages to discover multicast routers is insufficient due to query suppression. MRD therefore provides a standardized way to identify multicast routers without relying on any particular multicast routing protocol.

NOTE: The default values recommended in the MRD draft are implemented in the switch.

Multicast Router Discovery uses the following three message types to discover multicast routers:

- Multicast Router Advertisement – Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the occurrence of these events:
  - Upon the expiration of a periodic (randomized) timer.
  - As a part of a router's start up procedure.
  - During the restart of a multicast forwarding interface.
  - On receipt of a Solicitation message.
- Multicast Router Solicitation – Devices send Solicitation messages in order to solicit Advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an Advertisement.
- Multicast Router Termination – These messages are sent when a router stops IP multicast routing functions on an interface. Termination messages are sent by multicast routers when:
  - Multicast forwarding is disabled on an interface.
  - An interface is administratively disabled.
  - The router is gracefully shut down.

Advertisement and Termination messages are sent to the All-Snoopers multicast address. Solicitation messages are sent to the All-Routers multicast address.

NOTE: MRD messages are flooded to all ports in a VLAN where IGMP snooping or routing has been enabled. To ensure that older switches which do not support MRD can also learn the multicast router port, the switch floods IGMP general query packets, which do not have a null source address (0.0.0.0), to all ports in the attached VLAN. IGMP packets with a null source address are only flooded to all ports in the VLAN if the system is operating in multicast flooding mode, such as when a new VLAN or new router port is being established, or an spanning tree topology change has occurred. Otherwise, this kind of packet is only forwarded to known multicast routing ports.

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of configured VLANs. (Range: 1-4093)
- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

  When IGMP snooping is enabled globally (see page 277), the per VLAN interface settings for IGMP snooping take precedence.

  When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
- **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

  If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled)

  If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period. Note that this time out is set to Last Member Query Interval * Robustness Variable (fixed at 2) as defined in RFC 2236.

  If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

  This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.
- **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: Enabled)
- **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts. (Default: Disabled)

  By default, general query messages are flooded to all ports, except for the multicast router through which they are received.

  If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

- **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-2; Default: 2)

  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 2 are supported, and version 2 is backward compatible, so the switch can operate with other devices using either Version 1 or 2.

- **Last Member Query Interval** – The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second in multiples of 10; Default: 1 second)

  When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.

  A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic.

- **Last Member Query Count** – The number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. (Range: 1-255; Default: 2)

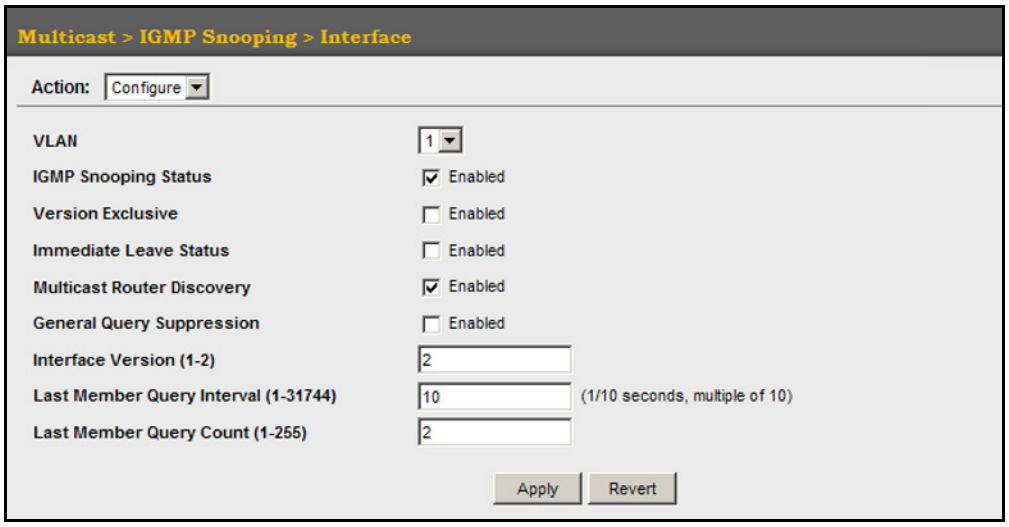
  This attribute will take effect only if IGMP querier is enabled.

WEB INTERFACE

To configure IGMP snooping on a VLAN:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure from the Action list.
3. Select the VLAN to configure and update the required parameters.
4. Click Apply.

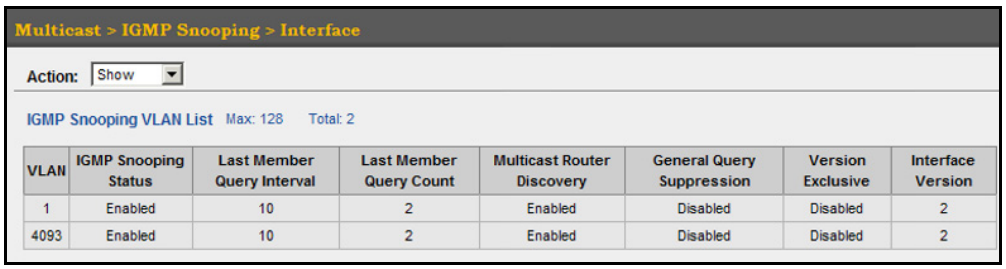
Figure 180: Configuring IGMP Snooping on an Interface


Multicast > IGMP Snooping > Interface
Action: Configure
VLAN 1
IGMP Snooping Status Enabled
Version Exclusive Enabled
Immediate Leave Status Enabled
Multicast Router Discovery Enabled
General Query Suppression Enabled
Interface Version (1-2) 2
Last Member Query Interval (1-31744) 10 (1/10 seconds, multiple of 10)
Last Member Query Count (1-255) 2
Apply
Revert

To show the interface settings for IGMP snooping:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Show from the Action list.

Figure 181: Showing Interface Settings for IGMP Snooping


Multicast > IGMP Snooping > Interface
Action: Show
IGMP Snooping VLAN List Max: 128 Total: 2
VLAN | IGMP Snooping Status | Last Member Query Interval | Last Member Query Count | Multicast Router Discovery | General Query Suppression | Version Exclusive | Interface Version
1 | Enabled | 10 | 2 | Enabled | Disabled | Disabled | 2
4093 | Enabled | 10 | 2 | Enabled | Disabled | Disabled | 2

DISPLAYING MULTICAST GROUPS DISCOVERED BY IGMP SNOOPING

Use the Multicast > IGMP Snooping > Forwarding Entry page to display the forwarding entries learned through IGMP Snooping.

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see page 277).

PARAMETERS

These parameters are displayed:

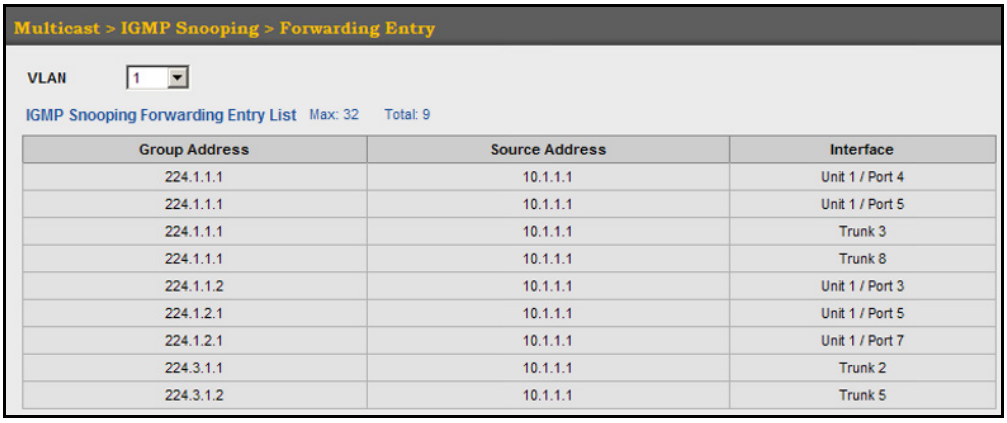
- **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Source Address** – The address of one of the multicast servers transmitting traffic to the specified group.
- **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.

WEB INTERFACE

To show multicast groups learned through IGMP snooping:

1. Click Multicast, IGMP Snooping, Forwarding Entry.
2. Select the VLAN for which to display this information.

Figure 182: Showing Multicast Groups Learned by IGMP Snooping


Multicast > IGMP Snooping > Forwarding Entry
VLAN 1
IGMP Snooping Forwarding Entry List Max: 32 Total: 9
Group Address
Source Address
Interface
224.1.1.1 10.1.1.1 Unit 1 / Port 4
224.1.1.1 10.1.1.1 Unit 1 / Port 5
224.1.1.1 10.1.1.1 Trunk 3
224.1.1.1 10.1.1.1 Trunk 8
224.1.1.2 10.1.1.1 Unit 1 / Port 3
224.1.2.1 10.1.1.1 Unit 1 / Port 5
224.1.2.1 10.1.1.1 Unit 1 / Port 7
224.3.1.1 10.1.1.1 Trunk 2
224.3.1.2 10.1.1.1 Trunk 5

FILTERING AND THROTTLING IGMP GROUPS

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more addresses, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

ENABLING IGMP FILTERING AND THROTTLING

Use the Multicast > IGMP Snooping > Filter (Configure General) page to enable IGMP filtering and throttling globally on the switch.

PARAMETERS

These parameters are displayed:

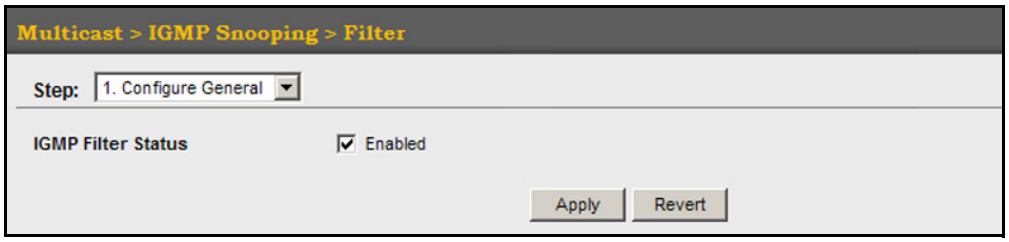
- **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

WEB INTERFACE

To enable IGMP filtering and throttling on the switch:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure General from the Step list.
3. Enable IGMP Filter Status.
4. Click Apply.

Figure 183: Enabling IGMP Filtering and Throttling



CONFIGURING IGMP FILTER PROFILES

Use the Multicast > IGMP Snooping > Filter (Add) page to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.

COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

PARAMETERS

These parameters are displayed:

Add

- **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)
- **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)

  When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range.

Add Multicast Group Range

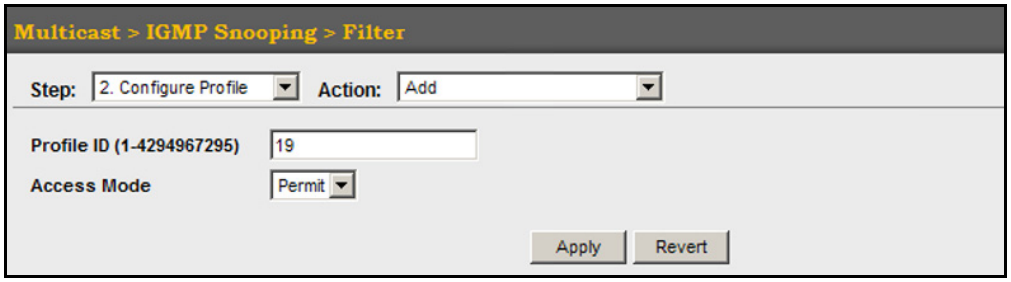
- **Profile ID** – Selects an IGMP profile to configure.
- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

WEB INTERFACE

To create an IGMP filter profile and set its access mode:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Add from the Action list.
4. Enter the number for a profile, and set its access mode.
5. Click Apply.

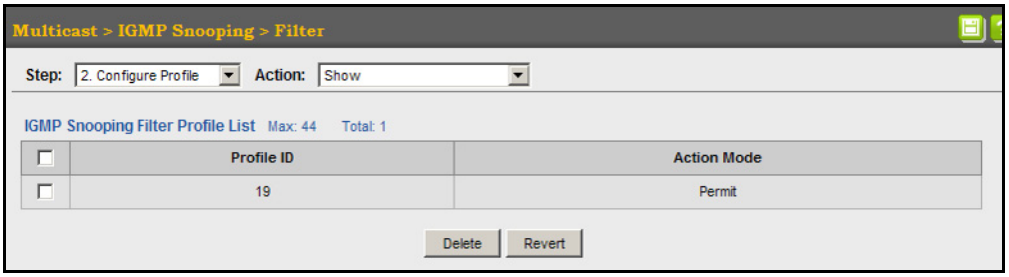
Figure 184: Creating an IGMP Filtering Profile



To show the IGMP filter profiles:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Show from the Action list.

Figure 185: Showing the IGMP Filtering Profiles Created

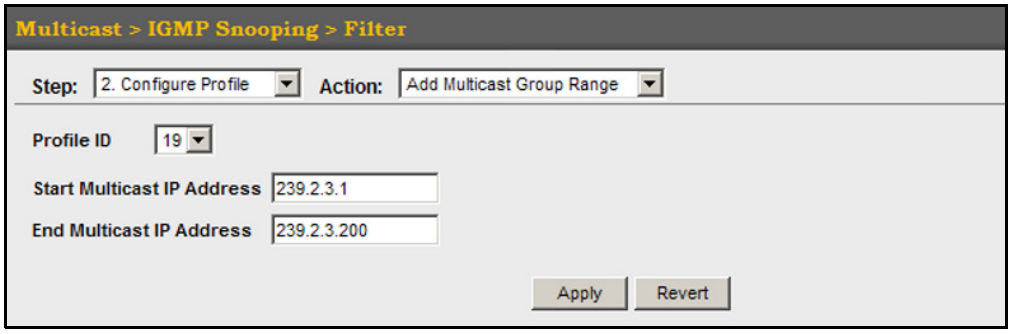


To add a range of multicast groups to an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Add Multicast Group Range from the Action list.
4. Select the profile to configure, and add a multicast group address or range of addresses.

5. Click Apply.

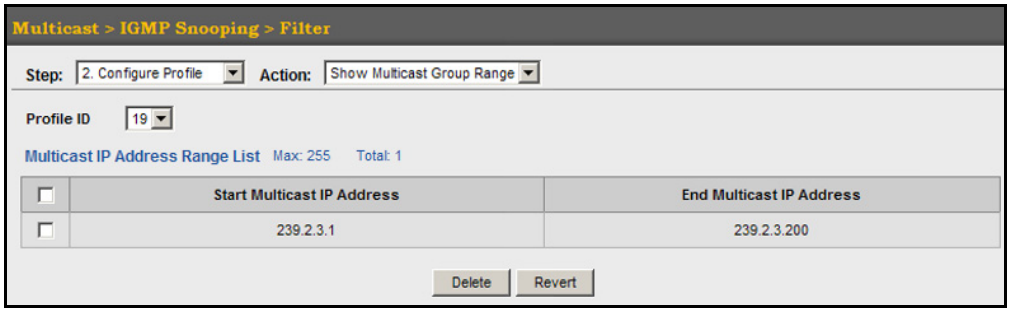
Figure 186: Adding Multicast Groups to an IGMP Filtering Profile



To show the multicast groups configured for an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Profile from the Step list.
3. Select Show Multicast Group Range from the Action list.
4. Select the profile for which to display this information.

Figure 187: Showing the Groups Assigned to an IGMP Filtering Profile



CONFIGURING IGMP FILTERING AND THROTTLING FOR INTERFACES

Use the Multicast > IGMP Snooping > Filter (Configure Interface) page to assign and IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

COMMAND USAGE

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

PARAMETERS

These parameters are displayed:

- **Interface** – Port or trunk identifier.

  An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.

- **Profile ID** – Selects an existing profile to assign to an interface.

- **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 0-255; Default: 255)

- **Current Multicast Groups** – Displays the current multicast groups the interface has joined.

- **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)
  - **Deny** - The new multicast group join report is dropped.
  - **Replace** - The new multicast group replaces an existing group.

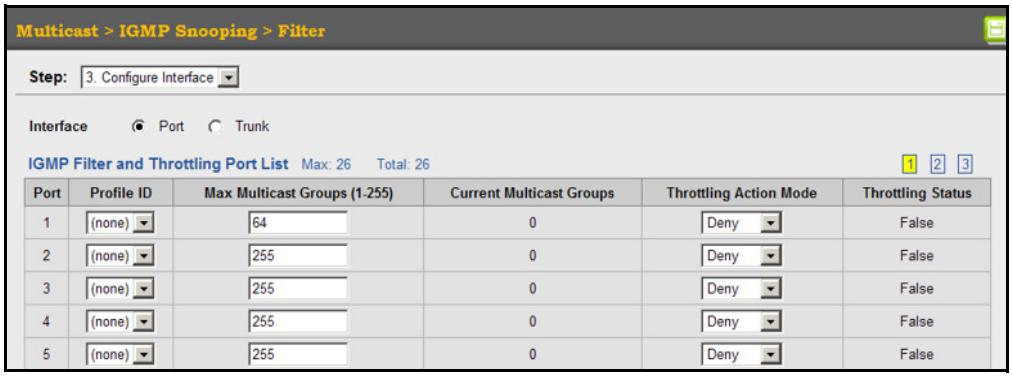
- **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

WEB INTERFACE

To configure IGMP filtering or throttling for a port or trunk:

1. Click Multicast, IGMP Snooping, Filter.
2. Select Configure Interface from the Step list.
3. Select a profile to assign to an interface, then set the maximum number of allowed multicast groups and the throttling response.
4. Click Apply.

Figure 188: Configuring IGMP Filtering and Throttling Interface Settings


Multicast > IGMP Snooping > Filter
Step: 3. Configure Interface
Interface Port Trunk
IGMP Filter and Throttling Port List Max: 26 Total: 26
1 2 3
Port
Profile ID
Max Multicast Groups (1-255)
Current Multicast Groups
Throttling Action Mode
Throttling Status
1 (none) 64 0 Deny False
2 (none) 255 0 Deny False
3 (none) 255 0 Deny False
4 (none) 255 0 Deny False
5 (none) 255 0 Deny False

SECTION III

APPENDICES

This section provides additional information and includes these items:

- "Software Specifications" on page 297
- "Troubleshooting" on page 301
- "License Information" on page 303

A SOFTWARE SPECIFICATIONS

SOFTWARE FEATURES

MANAGEMENT AUTHENTICATION	Local, RADIUS, TACACS+, Port Authentication (802.1X), HTTPS, Port Security, IP Filter
CLIENT ACCESS CONTROL	Access Control Lists (512 rules), Port Authentication (802.1X), Port Security
PORT CONFIGURATION	100BASE-TX: 10/100 Mbps, half/full duplex 100BASE-FX: 100 Mbps at full duplex (SFP) 1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex 1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP)
FLOW CONTROL	Full Duplex: IEEE 802.3-2005 Half Duplex: Back pressure
STORM CONTROL	Broadcast, multicast, or unicast traffic throttled above a critical threshold
PORT MIRRORING	26 sessions, one or more source ports to one destination port
RATE LIMITS	Input/Output Limits Range configured per port
PORT TRUNKING	Static trunks (Cisco EtherChannel compliant) Dynamic trunks (Link Aggregation Control Protocol)
SPANNING TREE ALGORITHM	Spanning Tree Protocol (STP, IEEE 802.1D-2004) Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004)

VLAN SUPPORT Up to 256 groups; port-based, tagged (802.1Q), voice VLANs

CLASS OF SERVICE Supports four levels of priority
Strict, Shaped Deficit Weighted Round Robin, or strict-WRR queuing
Layer 3/4 priority mapping: IP DSCP

QUALITY OF SERVICE DiffServ supports class maps, policy maps, and service policies

MULTICAST FILTERING IGMP Snooping (Layer 2)

ADDITIONAL FEATURES BOOTP Client
DHCP Client
DNS Client, Proxy
LLDP (Link Layer Discover Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SNMP (Simple Network Management Protocol)
SNTP (Simple Network Time Protocol)

MANAGEMENT FEATURES

IN-BAND MANAGEMENT Web-based HTTP or HTTPS, SNMP manager

SOFTWARE LOADING HTTP

SNMP Management access via MIB database
Trap management to specified hosts

RMON Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

STANDARDS

IEEE 802.1AB Link Layer Discovery Protocol
IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
  Spanning Tree Protocol
  Rapid Spanning Tree Protocol
IEEE 802.1p Priority tags

IEEE 802.1Q VLAN
IEEE 802.1X Port Authentication
IEEE 802.3-2005
Ethernet, Fast Ethernet, Gigabit Ethernet
Link Aggregation Control Protocol (LACP)
Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
DHCP Client (RFC 2131)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IPv4 IGMP (RFC 3228)
RADIUS+ (RFC 2618)
RMON (RFC 2819 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 1901, 2571)
SNMPv3 (RFC DRAFT 2273, 2576, 3410, 3411, 3413, 3414, 3415)
SNTP (RFC 2030)
TFTP (RFC 1350)

MANAGEMENT INFORMATION BASES

Bridge MIB (RFC 1493)
Differentiated Services MIB (RFC 3289)
DNS Resolver MIB (RFC 1612)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
Link Aggregation MIB (IEEE 802.3ad)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
P-Bridge MIB (RFC 2674P)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Power Ethernet MIB (RFC 3621)
Private MIB

Q-Bridge MIB (RFC 2674Q)
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMP Community MIB (RFC 3584)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMPv2 IP MIB (RFC 2011)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)

B TROUBLESHOOTING

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 28: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser, or SNMP software	◆ Be sure the switch is powered up. ◆ Check network cabling between the management station and the switch. ◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. ◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.
Forgot or lost the password	◆ Contact your local distributor.

USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Contact your distributor's service engineer.

C LICENSE INFORMATION

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

THE GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GLOSSARY

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DIFFSERV Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS Domain Name Service. A system used for translating host names for network nodes into IP addresses.

DSCP Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EAPOL Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

GMRP Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

IEEE 802.1D Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1P An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1W An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC Defines frame extensions for VLAN tagging.

IEEE 802.3X Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP QUERY On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP SNOOPING Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT Management of the network from a station attached directly to the network.

IP MULTICAST FILTERING A process whereby this switch can pass multicast traffic along to participating hosts.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LINK AGGREGATION *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MRD Multicast Router Discovery is a A protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

MULTICAST SWITCHING A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

PORT AUTHENTICATION *See IEEE 802.1X*.

PORT MIRRORING A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

PORT TRUNK Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

QOS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

INDEX

NUMERICS

802.1X
    authenticator, configuring 192
    global settings 191
    port authentication 189
    supplicant, configuring 196

A

acceptable frame type 97
ACL 175
    binding to a port 184
    IPv4 Extended 177, 179
    IPv4 Standard 177, 178
    MAC 177, 182
Address Resolution Protocol *See* ARP
address table 101
    aging time 103
    aging time, displaying 103
    aging time, setting 103
address, management access 31
ARP
    configuration 269
    description 268

B

BOOTP 271
BPDU 108
    selecting protocol based on message format 115
bridge extension capabilities, displaying 51
broadcast storm, threshold 123

C

cable diagnostics 75
canonical format indicator 136
class map, DiffServ 140
Class of Service *See* CoS
clustering switches, management access 261
committed burst size, QoS policy 147, 148, 149
committed information rate, QoS policy 147, 148, 149
community string 240
configuration files, restoring defaults 52
configuration settings
    restoring 54, 55
    saving 54
CoS 125
    configuring 125
    default mapping to internal values 136
    enabling 132
    layer 3/4 priorities 132
    priorities, mapping to internal values 136
    queue mapping 129
    queue mode 126
    queue weights, assigning 128
CoS/CFI to PHB/drop precedence 136
CPU
    status 61
    utilization, showing 61

D

default IPv4 gateway, configuration 271
default priority, ingress port 125
default settings, system 28
DHCP 271
    client 271
Differentiated Code Point Service *See* DSCP
Differentiated Services *See* DiffServ
DiffServ 139
    binding policy to interface 153
    class map 140
    classifying QoS traffic 140
    color aware, srTCM 148
    color aware, trTCM 149
    color blind, srTCM 148
    color blind, trTCM 149
    committed burst size 148, 150
    committed information rate 148, 149
    configuring 139
    conforming traffic, configuring response 147
    excess burst size 148
    metering, configuring 143, 144, 145
    peak burst size 150
    peak information rate 149
    policy map 143
    policy map, description 140, 147
    QoS policy 143
    service policy 153
    setting CoS for matching packets 147
    setting IP DSCP for matching packets 147
    setting PHB for matching packets 147
    single-rate, three-color meter 144, 148
    srTCM metering 144, 148
    traffic between CIR and BE, setting response 148
    traffic between CIR and PIR, setting response 149
    trTCM metering 149

two-rate, three-color meter 145
violating traffic, setting response 150
downloading software 52
drop precedence
CoS priority mapping 136
DSCP ingress map 134
DSCP 132
enabling 132
mapping to internal values 133
DSCP ingress map, drop precedence 134
DSCP to PHB/drop precedence 134
dynamic addresses
clearing 105
displaying 104
dynamic VLAN assignment 168, 169

E

edge port, STA 115, 117
engine ID 231, 232
event logging 201
excess burst size, QoS policy 148

F

firmware
displaying version 48
upgrading 52
version, displaying 48

G

gateway, IPv4 default 271
general security measures 161
GNU license 303

H

hardware version, displaying 48
HTTPS 172, 173
configuring 172
replacing SSL certificate 173
secure-site certificate 173
HTTPS, secure server 172

I

IEEE 802.1D 107
IEEE 802.1w 107
IEEE 802.1X 189
IGMP
filter profiles, binding to interface 293
filter profiles, configuration 291
filter, interface configuration 293
filter, parameters 291
filtering & throttling 290
filtering & throttling, enabling 290
filtering & throttling, interface configuration 293
filtering & throttling, status 290
filtering, configuring profile 291
filtering, creating profile 291
filtering, group range 291
groups, displaying 283
Layer 2 276
query 276, 277
services, displaying 289
snooping 276
snooping & query, parameters 277
snooping, configuring 277
snooping, enabling 277
snooping, immediate leave 286
IGMP snooping
configuring 284
enabling per interface 284, 286
forwarding entries 289
immediate leave, status 286
interface attached to multicast router 282
last member query count 287
last member query interval 287
querier timeout 279
router port expire time 279
static host interface 276
static multicast routing 280
static port assignment 282
static router interface 276
static router port, configuring 280
TCN flood 278
unregistered data flooding 279
version exclusive 279
version for interface, setting 287
version, setting 279
immediate leave, IGMP snooping 286
ingress filtering 97
IP filter, for management access 185
IPv4 address
BOOTP/DHCP 271
setting 267, 271

J

jumbo frame 50

L

LACP
configuration 80
group attributes, configuring 83
group members, configuring 81
local parameters 87
partner parameters 88
protocol message statistics 85
protocol parameters 80
last member query count, IGMP snooping 287
last member query interval, IGMP snooping 287
license information, GNU 303
Link Layer Discovery Protocol - Media Endpoint Discovery *See* LLDP-MED
Link Layer Discovery Protocol *See* LLDP

link type, STA 115, 117
LLDP 205
device statistics details, displaying 223
device statistics, displaying 221
display device information 214, 216
displaying remote information 216
interface attributes, configuring 208
local device information, displaying 214
message attributes 208
message statistics 221
remote information, displaying 221
remote port information, displaying 216
timing attributes, configuring 206
TLV 205, 208
TLV, 802.1 209
TLV, 802.3 209
TLV, basic 208
TLV, management address 208
TLV, port description 209
TLV, system capabilities 209
TLV, system description 209
TLV, system name 209
LLDP-MED 205
notification, status 208
TLV 210
TLV, extended PoE 210
TLV, inventory 210
TLV, location 210
TLV, MED capabilities 210
TLV, network policy 210
TLV, PoE 210
logging
messages, displaying 203
syslog traps 204
to syslog servers 204
log-in, web interface 35
logon authentication 166
encryption keys 165
RADIUS client 164
RADIUS server 164
sequence 162
settings 163, 164
TACACS+ client 163
TACACS+ server 163

M

main menu, web interface 39
management access
filtering per address 185
IP filter 185
management address, setting 31
Management Information Bases (MIBs) 299
matching class settings, classifying QoS traffic 141
media-type 66
memory
status 62
utilization, showing 62
mirror port
configuring 69
configuring local traffic 69
mirror trunk
configuring 89
configuring local traffic 89
multicast filtering 275
enabling IGMP snooping 277, 286
enabling IGMP snooping per interface 284
router configuration 280
multicast groups 283, 289
displaying 283, 289
static 282, 283
multicast router discovery 285
multicast router port, displaying 281
multicast services
configuring 282
displaying 283
multicast static router port 280
configuring 280
multicast storm, threshold 123
multicast, filtering and throttling 290

N

network access
dynamic VLAN assignment 169
port configuration 169
secure MAC information 170

P

passwords 31
administrator setting 166
path cost 117
method 109
STA 114, 117
peak burst size, QoS policy 149
peak information rate, QoS policy 149
per-hop behavior, DSCP ingress map 134
policing traffic, QoS policy 143, 147
policy map
description 147
DiffServ 143
port authentication 189
port power
displaying status 227
inline 226
inline status 227
maximum allocation 226
priority 226
showing main power 227
port priority
configuring 125
default ingress 125
STA 114
port security, configuring 187
ports
autonegotiation 66

broadcast storm threshold 123
capabilities 66
configuring 65
duplex mode 67
flow control 67
forced selection on combo ports 66
mirroring 69
mirroring local traffic 69
multicast storm threshold 123
speed 67
statistics 71
unknown unicast storm threshold 123
power budgets
port 226
port priority 226
power savings
configuring 91
enabling per port 91
priority, default port ingress 125
problems, troubleshooting 301
protocol migration 115
PVID, port native VLAN 97

Q

QoS 139
configuration guidelines 140
configuring 139
CoS/CFI to PHB/drop precedence 136
DSCP to PHB/drop precedence 133
matching class settings 141
PHB to queue 129
selecting DSCP, CoS 132
QoS policy
committed burst size 147, 148, 149
committed information rate 147, 148, 149
excess burst size 148
peak burst size 149
peak information rate 149
policing flow 143, 147
srTCM 144
srTCM police meter 148
trTCM 145
trTCM police meter 149
Quality of Service *See* QoS
queue mode, setting 126
queue weight, assigning to CoS 128

R

RADIUS
logon authentication 164
settings 164
rate limit
port 119
setting 119
remote logging 204
restarting the system 63
RMON 250
alarm, displaying settings 252
alarm, setting thresholds 250
event settings, displaying 255
response to alarm setting 253
statistics history, collection 255
statistics history, displaying 257
statistics, collection 258
statistics, displaying 259
RSTP 107
global settings, configuring 108
global settings, displaying 112
interface settings, configuring 113
interface settings, displaying 116

S

security, general measures 161
Simple Network Management Protocol *See* SNMP
single rate three color meter *See* srTCM
SNMP 227
community string 240
enabling traps 245
filtering IP addresses 185
global settings, configuring 230
trap manager 245
users, configuring 241, 243
SNMPv3
engine ID 231, 232
engine identifier, local 231
engine identifier, remote 232
groups 236
local users, configuring 241
remote users, configuring 243
user configuration 241, 243
views 233
SNTP
setting the system clock 58
specifying servers 59
software
displaying version 48
downloading 52
version, displaying 48
Spanning Tree Protocol *See* STA
specifications, software 297
srTCM
police meter 148
QoS policy 144
SSL, replacing certificate 173
STA 107
edge port 115, 117
forward delay 110
global settings, configuring 108
global settings, displaying 112
hello time 109
interface settings, configuring 113
interface settings, displaying 116
link type 115, 117
maximum age 110

path cost 114, 117
path cost method 109
port priority 114
protocol migration 115
transmission limit 109
standards, IEEE 298
startup files
creating 52
displaying 52
setting 52
static addresses, setting 101
statistics, port 71
STP 108
switch clustering, for management 261
switch settings
restoring 54
saving 54
system clock
setting 57
setting manually 57
setting the time zone 60
setting with SNTP 58
system logs 201
system software, downloading from server 52

T

TACACS+
logon authentication 163
settings 164
TCN
flood 278
general query solicitation 278
time zone, setting 60
time, setting 57
trap manager 245
troubleshooting 301
trTCM
police meter 149
QoS policy 145
trunk
configuration 77
LACP 80
static 78
trunks
mirroring 89
mirroring local traffic 89
two rate three color meter *See* trTCM
Type Length Value, *See* LLDP TLV

U

unknown unicast storm, threshold 123
unregistered data flooding, IGMP snooping 279
upgrading software 52
user account 166
user password 166

V

VLANs
acceptable frame type 97
adding static members 96
configuring port members, VLAN index 98
creating 95
description 93
displaying port members 98
displaying port members by interface 99
displaying port members by interface range 100
displaying port members by VLAN index 98
dynamic assignment 169
egress mode 96
ingress filtering 97
interface configuration 96
port members, displaying 98
PVID 97
voice 155
voice VLANs 155
detecting VoIP devices 156
enabling for ports 158
identifying client devices 157
VoIP traffic 155
ports, configuring 158
telephony OUI, configuring 157
voice VLAN, configuring 155
VoIP, detecting devices 159

W

web interface
configuration buttons 36
home page 35
menu list 39
panel display 37



CE

JUNE/2011/ISSUE 2.2